

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants : Akira Ogino, et al.
Serial No. : 09/351,399
For : INFORMATION-SIGNAL PLAYBACK SYSTEM,
INFORMATION-SIGNAL READING APPARATUS,
INFORMATION-SIGNAL PROCESSING APPARATUS,
INFORMATION-SIGNAL PLAYBACK METHOD,
INFORMATION-SIGNAL READING METHOD AND
INFORMATION-SIGNAL PROCESSING APPARATUS
Filed : July 13, 1999
Examiner : Reagan, James A.
Art Unit : 3621
Confirmation No. : 9658

RECEIVED

APR 05 AM '00

GROUP 3600

745 Fifth Avenue
New York, NY 10151

EXPRESS MAIL

Mailing Label Number: EV 384276836 US

Date of Deposit: March 21, 2005

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" Service under 37 CFR 1.10 on the date indicated above and is addressed to: Board of Patent Appeals and Interferences, Assistant Commissioner for Patents, Washington, DC 20231.

Barnet Shindler
(Typed or printed name of person mailing paper or fee)

Barnet Shindler
(Signature of person mailing paper or fee)

RECEIVED
2005 MAR 29 AM 10:56
BOARD OF PATENT APPEALS
AND INTERFERENCES

APPELLANTS' REPLY BRIEF

Board of Patent Appeals and Interferences
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

This is a reply to the Examiner's Answer mailed on January 24, 2005.

RESPONSE TO EXAMINER'S ANSWER

In the Examiner's Answer of January 24, 2005, the Examiner states at page 3 that "The following is a NEW ground(s) of rejection, and is applicable to the appealed claims." Appellants respectfully disagree.

Appellants respectfully submit that a new ground(s) of rejection is not permissible by the Examiner. Specifically, section 1208, pages 1200-15 to 1200-16 in the Manual of Patent Examining Procedure (MPEP) state that "An examiner's answer **must not** include a new ground of rejection..." (emphasis added). Therefore, the 35 U.S.C. 103(a) rejection under U.S. Patent No. 6,226,618 to Downs et al. is **not** a proper reference.

Furthermore, even if the Examiner could apply Downs as a reference, Appellants submit that Downs is not a proper reference because the present application has an effective filing date, which antedates the filing date of Downs.

In particular, in explaining the 103(a) rejection with regard to claims 1-5, 13-15, 20-24, 32-36, 44-46 and 51-55, the Examiner acknowledged at page 6 of the Examiner's Answer that JP '662, Schneck and Ryan do not disclose "comparing means for comparing the decrypted information on said copyright protection with the unencrypted information on said copyright protection to judge if an attempt to alter the information on said copyright protection has been performed..." In an attempt to overcome this deficiency, the Examiner relied on Downs (and, in particular, column 15, line 58 to column 16, line 50) to teach such feature.

Downs was filed on August 13, 1998. The present application, on the other hand, has claimed priority under 35 U.S.C. 119 based upon Japanese Application No. 10-200264 filed on July 15, 1998 in Japan. A certified translation in English of this priority application (i.e., Japanese Application No. 10-200264) accompanies this Reply Brief. Accordingly, the present application has an effective filing date, which antedates the filing date of Downs. As a result, it is respectfully submitted that Downs is not an effective prior art reference against the present application.

Furthermore, although the applicant has asserted that Downs is not an effective reference against the present application, such assertion is not a representation concerning distinctions and/or similarities between the present invention and Downs. Applicants reserve the right to traverse any further rejection that may be presented on a similar document and having an earlier effective date.

Accordingly, withdrawal of the rejection to claims 1-5, 13-15, 20-24, 32-36, 44-46 and 51-55 is respectfully requested.

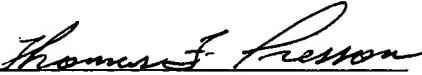
The Examiner has continually failed to present a reference, or combination of references that discloses a "comparing means for comparing the decrypted information on said copyright protection with the unencrypted information on said copyright protection to judge if an attempt to alter the information on said copyright protection has been performed..." Appellants therefore submit that the claims at issue in this Appeal are patentable over the prior art of record relied upon by the Examiner.

CONCLUSION

It is respectfully submitted that the Examiner erred in rejecting claims 1-5, 13-15, 20-24, 32-36, 44-46 and 51-55. Appellants request a reversal of these rejections by this Honorable Board. The Examiner's rejections and materials set forth in the Examiner's Reply should be reversed and allowance of this application should be mandated.

Respectfully submitted,

FROMMER, LAWRENCE & HAUG LLP
Attorneys for Appellants

By 

Thomas F. Presson
Registration No. 41,442
(212) 588-0800

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants : Akira Ogino, et al.
Serial No. : 09/351,399
For : INFORMATION-SIGNAL PLAYBACK SYSTEM,
INFORMATION-SIGNAL READING APPARATUS,
INFORMATION-SIGNAL PROCESSING APPARATUS,
INFORMATION-SIGNAL PLAYBACK METHOD,
INFORMATION-SIGNAL READING METHOD AND
INFORMATION-SIGNAL PROCESSING APPARATUS
Filed : July 13, 1999
Examiner : Reagan, James A.
Art Unit : 3621
Confirmation No. : 9658

745 Fifth Avenue
New York, NY 10151

EXPRESS MAIL

Mailing Label Number: EV 384276836 US

Date of Deposit: March 21, 2005

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" Service under 37 CFR 1.10 on the date indicated above and is addressed to: Board of Patent Appeals and Interferences, Assistant Commissioner for Patents, Washington, DC 20231.

Barnet Shindelman
(Typed or printed name of person mailing paper or fee)

(Signature of person mailing paper or fee)

PETITION TO HAVE A NEW GROUND OF REJECTION WITHDRAWN IN AN
EXAMINER'S ANSWER

Board of Patent Appeals and Interferences
Assistant Commissioner for Patents
Washington, D.C. 20231
Dear Sir:

This is a Petition to request withdrawal of a new ground of rejection in an Examiner's Answer in the above-identified application.

RECEIVED
2005 MAR 29 AM 10:57
BOARD OF PATENT APPEALS
AND INTERFERENCES

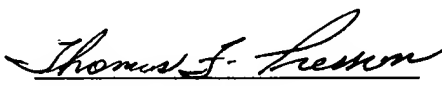
In the Examiner's Answer of January 24, 2005, the Examiner states at page 3 that "The following is a NEW ground(s) of rejection, and is applicable to the appealed claims." Appellants respectfully disagree.

Appellants respectfully submit that a new ground(s) of rejection is not permissible by the Examiner. Specifically, section 1208, pages 1200-15 to 1200-16 in the Manual of Patent Examining Procedure (MPEP) state that "An examiner's answer **must not** include a new ground of rejection..." (emphasis ours). Therefore, the 35 U.S.C. 103(a) rejection under U.S. Patent No. 6,226,618 to Downs et al. is **not** a proper reference.

Petitioner respectfully requests that the new ground of rejection in the Examiner's Answer be withdrawn.

It is believed that no fee is due for this Petition, but if it is deemed to be otherwise, then the Commissioner is authorized to charge our Deposit Account No. 50-0320.

Respectfully submitted,
FROMMER LAWRENCE & HAUG LLP

By: 
Thomas F. Presson
Reg. No. 41,442
(212) 588-0800

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANTS: Akira Ogino et al

SERIAL NO.: 09/351,399

GROUP ART UNIT: 3621

FILING DATE: July 13, 1999

EXAMINER: James A. REAGAN

TITLE: INFORMATION-SIGNAL PLAYBACK SYSTEM,
INFORMATION-SIGNAL READING APPARATUS, INFORMATION-SIGNAL
PROCESSING APPARATUS, INFORMATION-SIGNAL PLAYBACK METHOD,
INFORMATION-SIGNAL READING METHOD AND INFORMATION-SIGNAL
PROCESSING APPARATUS

Hon. Commissioner of Patents and Trademarks,
Washington, D.C. 20231

S I R:

CERTIFIED TRANSLATION

I, Masaaki Iwami of 3-22, Asagaya-minami 1-chome, Suginami-ku, Tokyo, Japan, am an experienced translator of the Japanese language into the English language and I hereby certify that the attached comprises an accurate translation into English of Japanese Patent Application No. H10-200264 filed July 15, 1998.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

March 10, 2005

Date


Masaaki IWAMI

RECEIVED
29 MAR 29 AM 10:57
DEPT OF PATENT APPEALS
AND INTERFERENCES

【Document Name】 Application for Patent

【Reference No.】 9800397612

【Application Date】 July 15, 1998

【Destination】 Commissioner, Patent Office

【International Patent Classification】 H04L 9/12

【Title of the Invention】 INFORMATION-SIGNAL REPRODUCING
SYSTEM, INFORMATION-SIGNAL READING APPARATUS,
INFORMATION-SIGNAL PROCESSING APPARATUS, INFORMATION-SIGNAL
REPRODUCING METHOD, INFORMATION-SIGNAL READING METHOD AND
INFORMATION-SIGNAL PROCESSING APPARATUS

【Number of Claims】 62

【Inventor】

 【Address】 c/o Sony Corporation
 7-35, Kitashinagawa 6-chome,
 Shinagawa-ku, Tokyo

 【Name】 Akira Ogino

【Inventor】

 【Address】 c/o Sony Corporation
 7-35, Kitashinagawa 6-chome,
 Shinagawa-ku, Tokyo

 【Name】 Yuji Kimura

【Inventor】

 【Address】 c/o Sony Corporation
 7-35, Kitashinagawa 6-chome,
 Shinagawa-ku, Tokyo

 【Name】 Tadashi Ezaki

【Inventor】

【Address】 c/o Sony Corporation
7-35, Kitashinagawa 6-chome,
Shinagawa-ku, Tokyo

【Name】 Teruhiko Koori

【Applicant for Patent】

【Identification No.】 000002185

【Name】 Sony Corporation

【Representative】 Nobuyuki Idei

【Agent】

【Identification No.】 100091546

【Patent Attorney】

【Name】 Masami Satoh

【Telephone No.】 03-5386-1775

【Designation of Charge】

【Ledger No. for Prepayment】 048851

【Amount of Payment】 21,000 yen

【List of Filed Document】

【Object Name】 Specification 1

【Object Name】 Drawing 1

【Object Name】 Abstract 1

【Number of Comprehensive Power of Attorney】 9710846

【Necessity of Confirmation】 Necessary

[Name of Document] Specification

[Title of the Invention] INFORMATION-SIGNAL REPRODUCING
SYSTEM, INFORMATION-SIGNAL READING APPARATUS,
INFORMATION-SIGNAL PROCESSING APPARATUS, INFORMATION-
SIGNAL REPRODUCING METHOD, INFORMATION-SIGNAL READING
METHOD AND INFORMATION-SIGNAL PROCESSING APPARATUS

[What is Claimed is]

[Claim 1] An information-signal reproducing system
comprising an information-signal reading apparatus for
reading out a main information signal and information on
copyright protection from a recording medium containing
said main information signal and information on at least
copyright protection, and an information-signal
processing apparatus for receiving said main information
signal and said information on copyright protection
received from said information-signal reading apparatus,
wherein said information-signal reading apparatus
has:

readout means for reading out said information on
copyright protection from said recording medium;

encryption means for encrypting said information on
copyright protection read out by said readout means; and

output means for supplying said information on
copyright protection encrypted by said encryption means

and said unencrypted information on copyright protection to said information-signal processing apparatus, and

said information-signal processing apparatus has:

decryption means for decrypting said encrypted information on copyright protection received from said information-signal reading apparatus; and

control means for controlling predetermined processing carried out on said main information signal on the basis of said unencrypted information on copyright protection received from said information-signal reading apparatus and information on copyright protection obtained as a result of decryption carried out by said decryption means.

[Claim 2] The information-signal reproducing system according to claim 1 wherein said information on copyright protection is media-type information indicating the type of said recording medium.

[Claim 3] The information-signal reproducing system according to claim 1 wherein said encryption means employed in said information-signal reading apparatus encrypts said information on copyright protection in accordance with a CSS system.

[Claim 4] The information-signal reproducing system according to claim 1 wherein:

additional information for controlling a copy operation has been added to said main information signal recorded on said recording medium;

said information-signal processing apparatus is provided with an additional-information detecting means for detecting said additional information added to said main information signal received from said information-signal reading apparatus; and

said control means controls predetermined processing carried out on said main information signal by taking said additional information detected by said information-signal detecting means into consideration.

[Claim 5] The information-signal reproducing system according to claim 4 wherein:

said additional information is information superposed on said main information signal as digital-watermark information; and

said additional-information detecting means employed in said information-signal processing apparatus detects said digital-watermark information superposed on said main information signal.

[Claim 6] An information-signal reproducing system comprising an information-signal reading apparatus for reading out a main information signal and information on

copyright protection from a recording medium containing said main information signal and information on at least copyright protection, and an information-signal processing apparatus for receiving said main information signal and said information on copyright protection received from said information-signal reading apparatus, wherein said information-signal reading apparatus has:

readout means for reading out said information on copyright protection from said recording medium;

encryption means for encrypting said information on copyright protection read out by said readout means;

output means for supplying said information on copyright protection encrypted by said encryption means and said unencrypted information on copyright protection to said information-signal processing apparatus; and

readout control means for controlling an operation to read out said main information signal from said recording medium in accordance with a readout-control signal received from said information-signal processing apparatus, and

said information-signal processing apparatus has:

decryption means for decrypting said encrypted information on copyright protection received from said

information-signal reading apparatus; and

readout-control-signal generating means for generating said readout-control signal based on said unencrypted information on copyright protection received from said information-signal reading apparatus and information on copyright protection obtained as a result of decryption carried out by said decryption means and for supplying said readout-control signal to said information-signal reading apparatus.

[Claim 7] The information-signal reproducing system according to claim 6 wherein:

said information-signal processing apparatus is provided with a readout-control-signal encrypting means for encrypting a readout-control signal generated by said readout-control-signal generating means; and

said information-signal reading apparatus is provided with control-information decrypting means for receiving and decrypting encrypted a readout-control signal received from said information-signal processing apparatus.

[Claim 8] The information-signal reproducing system according to claim 6 wherein said information on copyright protection is media-type information indicating the type of said recording medium.

[Claim 9] The information-signal reproducing system according to claim 6 wherein said encryption means employed in said information-signal reading apparatus encrypts said information on copyright protection in accordance with a CSS system.

[Claim 10] The information-signal reproducing system according to claim 7 wherein said readout-control-signal encrypting means employed in said information-signal processing apparatus carries out encryption processing in accordance with a system different from a system adopted by said encryption means employed in said information-signal reading apparatus.

[Claim 11] The information-signal reproducing system according to claim 6 wherein:

additional information for controlling a copy operation has been added to said main information signal recorded on said recording medium;

said information-signal processing apparatus is provided with additional-information detecting means for detecting said additional information added to said main information signal received from said information-signal reading apparatus; and

said readout-control-signal generating means generates a readout-control signal to be supplied to said

information-signal reading apparatus by taking said additional information detected by said additional-information detecting means into consideration.

[Claim 12] The information-signal reproducing system according to claim 11 wherein:

said additional information is information superposed on said main information signal as digital-watermark information; and

said additional-information detecting means employed in said information-signal processing apparatus detects said digital-watermark information superposed on said main information signal.

[Claim 13] An information-signal reading apparatus for reading out a main information signal and information on copyright protection from a recording medium containing said main information signal and information on at least copyright protection and for supplying said signal and said information to an information-signal processing apparatus, said information-signal reading apparatus comprising:

readout means for reading out said information on copyright protection from said recording medium;

encryption means for encrypting said information on copyright protection read out by said readout means; and

output means for supplying said information on copyright protection encrypted by said encryption means and said unencrypted information on copyright protection to said information-signal processing apparatus.

[Claim 14] The information-signal reading apparatus according to claim 13 wherein said information on copyright protection is media-type information indicating the type of said recording medium.

[Claim 15] The information-signal reading apparatus according to claim 13 wherein said encryption means employed in said information-signal reading apparatus encrypts said information on copyright protection in accordance with a CSS system.

[Claim 16] An information-signal reading apparatus for reading out a main information signal and information on copyright protection from a recording medium containing said main information signal and information on at least copyright protection and for supplying said signal and said information to an information-signal processing apparatus, said information-signal reading apparatus comprising:

readout means for reading out said information on copyright protection from said recording medium;

encryption means for encrypting said information on

copyright protection read out by said readout means;

output means for supplying said information on copyright protection encrypted by said encryption means and said unencrypted information on copyright protection to said information-signal processing apparatus; and

readout control means for controlling an operation to read out said main information signal from said recording medium in accordance with a readout-control signal received from said information-signal processing apparatus.

[Claim 17] The information-signal reading apparatus according to claim 16 wherein:

said readout-control signal generated by said information-signal processing apparatus is encrypted information; and

control-information decrypting means is provided for decrypting said encrypted readout-control signal.

[Claim 18] The information-signal reading apparatus according to claim 16 wherein said information on copyright protection is media-type information indicating the type of said recording medium.

[Claim 19] The information-signal reading apparatus according to claim 16 wherein said encryption means employed in said information-signal reading apparatus

encrypts said information on copyright protection in accordance with a CSS system.

[Claim 20] An information-signal processing apparatus for receiving a main information signal, encrypted information on copyright protection and unencrypted information on copyright protection, said information-signal processing apparatus comprising:

decryption means for decrypting said encrypted information on copyright protection; and

control means for controlling predetermined processing carried out on said main information signal on the basis of said unencrypted information on copyright protection and information on copyright protection obtained as a result of decryption carried out by said decryption means.

[Claim 21] The information-signal processing apparatus according to claim 20 wherein said information on copyright protection is media-type information indicating the type of said recording medium.

[Claim 22] The information-signal processing apparatus according to claim 20 wherein said encrypted information on copyright protection is information encrypted in accordance with a CSS system.

[Claim 23] The information-signal processing apparatus

according to claim 20 wherein:

additional information for controlling a copy operation has been added to said main information signal;

additional-information detecting means is provided for detecting said additional information added to said main information signal; and

said control means controls an operation to output said main information signal by taking said additional information detected by said information-signal detecting means into consideration.

[Claim 24] The information-signal processing apparatus according to claim 23 wherein:

said additional information is information superposed on said main information signal as digital-watermark information; and

said additional-information detecting means detects said digital-watermark information superposed on said main information signal.

[Claim 25] An information-signal processing apparatus for receiving a main information signal, encrypted information on copyright protection and unencrypted information on copyright protection , said information-signal processing apparatus comprising:

decryption means for decrypting said encrypted

information on copyright protection; and

control-signal generating means for generating control signal based on said unencrypted information on copyright protection and information on copyright protection obtained as a result of decryption carried out by said decryption means and for supplying said control signal to a supplier of said main information signal.

[Claim 26] The information-signal processing apparatus according to claim 25 wherein:

control-signal encrypting means is provided for encrypting control signal generated by said control-signal generating means; and

said encrypted control signal is supplied to a supplier of said main information signal.

[Claim 27] The information-signal processing apparatus according to claim 25 wherein said information on copyright protection is media-type information indicating the type of said recording medium.

[Claim 28] The information-signal processing apparatus according to claim 25 wherein said information on copyright protection has been encrypted in accordance with a CSS system.

[Claim 29] The information-signal processing apparatus according to claim 26 wherein said information on

copyright protection has been encrypted in accordance with a system different from a system adopted by said control-signal encrypting means.

[Claim 30] The information-signal processing apparatus according to claim 25 wherein:

additional information for controlling a copy operation has been added to said main information signal recorded on said recording medium;

additional-information detecting means is provided for detecting said additional information added to said main information signal; and

said control-signal generating means generates a control signal by taking said additional information detected by said additional-information detecting means into consideration.

[Claim 31] The information-signal processing apparatus according to claim 30 wherein:

said additional information is information superposed on said main information signal as digital-watermark information; and

said additional-information detecting means detects said digital-watermark information superposed on said main information signal.

[Claim 32] An information-signal reproducing method for

driving an information-signal reading apparatus to read out a main information signal and information on copyright protection from a recording medium containing said main information signal and information on at least copyright protection and supply said main information signal and said information on copyright protection to an information-signal processing apparatus, said information-signal reproducing method comprising the steps of:

driving said information-signal reading apparatus to supply encrypted information on copyright protection and unencrypted information on copyright protection to said information-signal processing apparatus; and

driving said information-signal processing apparatus to decrypt said encrypted information on copyright protection received from said information-signal reading apparatus, and controls predetermined processing carried out on said main information signal on the basis of said unencrypted information on copyright protection received from said information-signal reading apparatus and information on copyright protection obtained as a result of decryption.

[Claim 33] The information-signal reproducing method according to claim 32 wherein said information on

copyright protection is media-type information indicating the type of said recording medium.

[Claim 34] The information-signal reproducing method according to claim 32 further including the step of encrypting said information on copyright protection in accordance with a CSS system.

[Claim 35] The information-signal reproducing method according to claim 32;

wherein additional information for controlling a copy operation has been added to said main information signal recorded on said recording medium, said information-signal reproducing method further including the step of driving said information-signal processing apparatus to detect said additional information added to said main information signal and control predetermined processing carried out on said main information signal by taking said detected additional information into consideration.

[Claim 36] The information-signal reproducing method according to claim 35;

wherein said additional information is information superposed on said main information signal as digital-watermark information, said information-signal reproducing method further including the step of driving

said information-signal processing apparatus to detect said digital-watermark information superposed on said main information signal.

[Claim 37] An information-signal reproducing method for driving an information-signal reading apparatus to read out a main information signal and information on copyright protection from a recording medium containing said main information signal and information on at least copyright protection and supply said main information signal and said information on copyright protection to an information-signal processing apparatus, said information-signal reproducing method comprising the steps of:

driving said information-signal reading apparatus to supply encrypted information on copyright protection and unencrypted information on copyright protection to said information-signal processing apparatus and control an operation to read out said main information signal from said recording medium on the basis of a readout-control signal received from said information-signal processing apparatus; and

driving said information-signal processing apparatus to decrypt said encrypted information on copyright protection received from said information-

signal reading apparatus, generate said readout-control signal on the basis of said unencrypted information on copyright protection received from said information-signal reading apparatus and information on copyright protection obtained as a result of decryption, and supply said readout-control signal to said information-signal reading apparatus.

[Claim 38] The information-signal reproducing method according to claim 37 further including the steps of:

driving said information-signal processing apparatus to encrypt said readout-control signal and supply said encrypted readout-control signal to said information-signal reading apparatus; and

driving said information-signal reading apparatus to decrypt said encrypted read-out control signal received from said information-signal processing apparatus.

[Claim 39] The information-signal reproducing method according to claim 37 wherein said information on copyright protection is media-type information indicating the type of said recording medium.

[Claim 40] The information-signal reproducing method according to claim 37 further including the step of encrypting said information on copyright protection in

accordance with a CSS system.

[Claim 41] The information-signal reproducing method according to claim 37 further including the steps of:

encrypting said information on copyright protection in accordance with a predetermined system; and

encrypting said readout control signal in accordance with a system different from said predetermined system.

[Claim 42] The information-signal reproducing method according to claim 37,

wherein additional information for controlling a copy operation has been added to said main information signal recorded on said recording medium, said information-signal reproducing method further including the step of driving said information-signal processing apparatus to:

detect said additional information added to said main information signal received from said information-signal reading apparatus; and

generate a readout-control signal by taking said detected additional information into consideration.

[Claim 43] The information-signal reproducing method according to claim 42,

wherein said additional information is information

superposed on said main information signal as digital-watermark information, said information-signal reproducing method further including the step of driving said information-signal processing apparatus to detect said digital-watermark information superposed on said main information signal.

[Claim 44] An information-signal reading method for reading out a main information signal and information on copyright protection from a recording medium containing said main information signal and information on at least copyright protection and for supplying said signal and said information to an information-signal processing apparatus, said information-signal reading method comprising the step of supplying encrypted information on copyright protection and said unencrypted information on copyright protection to said information-signal processing apparatus.

[Claim 45] The information-signal reading method according to claim 44 wherein said information on copyright protection is media-type information indicating the type of said recording medium.

[Claim 46] The information-signal reading method according to claim 44 further including the step of encrypting said information on copyright protection in

accordance with a CSS system.

[Claim 47] The An information-signal reading method for reading out a main information signal and information on copyright protection from a recording medium containing said main information signal and information on at least copyright protection and for supplying said signal and said information to an information-signal processing apparatus, said information-signal reading method comprising the steps of:

supplying encrypted information on copyright protection and unencrypted information on copyright protection to said information-signal processing apparatus; and

controlling an operation to read out said main information signal from said recording medium in accordance with a readout-control signal received from said information-signal processing apparatus.

[Claim 48] The information-signal reading method according to claim 47,

wherein said readout-control signal supplied from said information-signal processing apparatus is encrypted information, said information-signal reading method further including the step of decrypting said encrypted readout-control signal.

[Claim 49] The information-signal reading method according to claim 47 wherein said information on copyright protection is media-type information indicating the type of said recording medium.

[Claim 50] The information-signal reading method according to claim 47 wherein said information on copyright protection is information encrypted in accordance with a CSS system.

[Claim 51] An information-signal processing method for receiving a main information signal, encrypted information on copyright protection and unencrypted information on copyright protection, said information-signal processing method comprising the steps of:

decrypting said encrypted information on copyright protection; and

controlling predetermined processing carried out on said main information signal on the basis of said unencrypted information on copyright protection and decrypted information on copyright protection.

[Claim 52] The information-signal processing method according to claim 51 wherein said information on copyright protection is media-type information indicating the type of said recording medium.

[Claim 53] The information-signal processing method

according to claim 51 wherein said encrypted information on copyright protection is information encrypted in accordance with a CSS system.

[Claim 54] The information-signal processing method according to claim 51 wherein additional information for controlling a copy operation has been added to said main information signal, said information-signal processing method further including the steps of:

detecting said additional information added to said main information signal;

controlling predetermined processing carried out on said main information signal by taking said detected additional information into consideration.

[Claim 55] The information-signal processing method according to claim 54 wherein said additional information is information superposed on said main information signal as digital-watermark information, said information-signal processing method further including the step of detecting said digital-watermark information superposed on said main information signal.

[Claim 56] An information-signal processing method for receiving a main information signal, encrypted information on copyright protection and unencrypted information on copyright protection, said information-

signal processing method comprising the steps of:

decrypted said encrypted information on copyright protection; and

generating a control signal based on said unencrypted information on copyright protection and decrypted information on copyright protection and supplying said control signal to a supplier of said main information signal.

[Claim 57] The information-signal processing method according to claim 56 further including the steps of:

encrypting said control signal generated by said control-signal generating means; and

supplying said encrypted control signal to a supplier of said main information signal.

[Claim 58] The information-signal processing method according to claim 56 wherein said information on copyright protection is media-type information indicating the type of said recording medium.

[Claim 59] The information-signal processing method according to claim 56 wherein said encrypted information on copyright protection is information encrypted in accordance with a CSS system.

[Claim 60] The information-signal processing method according to claim 57 further including the step of

encrypting said control signal in accordance with a system different from a system, in which said information on copyright protection is encrypted.

[Claim 61] The information-signal processing method according to claim 56 wherein additional information for controlling a copy operation has been added to said main information signal, said information-signal processing method further including the steps of:

detecting said additional information added to said main information signal; and

generating said control signal by taking said detected additional information into consideration.

[Claim 62] The information-signal processing method according to claim 56 wherein said additional information is information superposed on said main information signal as digital-watermark information, said information-signal processing method further including the step of detecting said digital-watermark information superposed on said main information signal.

[Detailed Description of the Invention]

[0001]

[Technical Field to which the Invention Pertains]

The present invention relates to an information-

signal reproducing system, an information-signal reading apparatus, an information-signal processing apparatus, an information-signal reproducing method, an information-signal reading method and an information-signal processing method for protecting the copyright of an information signal recorded on recording media such as a DVD (Digital Video Disc) for presenting the information signal to the user or an information signal transmitted through transmission media such as the Internet and for preventing an illegal copy of such an information signal from being produced.

[0002]

With popularization of digital contents transmitted through the Internet and recorded on a digital video disk going on in recent years, infringement of a copyright granted to authors of digital contents in the form of an illegal copy of the digital contents becomes a problem. In order to solve the problem, there is a conceivable technique for preventing an illegal copy of digital contents from being produced. The technique uses information added to the digital contents for controlling copies of the digital contents.

[0003]

With regard to prevention of an illegal copy from

being produced, one can conceive a control implementation whereby a copy is not allowed at all and another control implementation in which a copy produced from an original source is allowed, but not of a copy produced from a copy in dependence on a source on which the copy prevention control is to be implemented. The latter is also referred to as a generation-limited copy control system. The former is applied to original software produced and sold by a content maker such as contents of a DVD-ROM. On the other hand, the generation-limited copy control system is applied to, among others, information transmitted through broadcasting media.

[0004]

In the case of the generation-limited copy control system, a system capable of controlling copy generations is desirable. As a system of information on copy control capable of controlling copy generations, there have been proposed a CGMS (Copy Generation Management System) and a system using digital-watermark processing.

[0005]

The digital-watermark processing is processing to embed information as noise into a part of picture data or music data which is trivial to the perception of a human being or a non-redundant part of a piece of music or a

picture. Additional information embedded in such digital-watermark processing into picture or music data is difficult to extract from the data. On the other hand, it is possible to detect additional information embedded in such digital-watermark processing into picture or music data from the data even after the data has been subjected to a filtering process or data compression.

[0006]

In the case of a copy control system using digital-watermark processing, additional information to be embedded into picture or music data indicates one of the following four control implementations:

- (1) Copy Free (allowing copies to be produced freely)
- (2) One Copy (allowing only the first copy generation to be produced)
- (3) No More Copy (allowing no subsequent copy generations)
- (4) Never Copy (absolutely allowing no copy)

The above control implementations represent restrictions of copy generations and copies of the picture or music data on which information is superposed by the digital-watermark processing.

[0007]

In the copy-free control implementation, music or

picture data can be copied freely. In the one-copy control implementation, only the first copy generation of music or picture data can be produced. The no-more-copy control implementation is applied to music or picture data of the first copy generation which has been produced in compliance with the one-copy control implementation (the second control implementation). With the no-more-copy control implementation, music or picture data of the first copy generation is prohibited from copying. The never-copy control implementation (the fourth control implementation) does not allow a copy to be produced at all.

[0008]

If digital-watermark information superposed on picture or music data indicates the one-copy control implementation, a recording apparatus conforming digital-watermark processing (that is, conforming to copy-restriction processing) will find out that the picture or music data can be copied and recorded, and thus record a copy of the data. However, the recording apparatus will update the digital-watermark information to information indicating the no-more-copy control implementation and superpose the updated information on the recorded data. If digital-watermark information superposed on picture or

music data to be dubbed indicates the no-more-copy control implementation, on the other hand, a recording apparatus conforming digital-watermark processing will determine that an operation to copy and record the picture or music data thereof is prohibited and inhibit a recording operation.

[0009]

The CGMS system is a system in which 2-bit additional information for copy control is superposed on one specific horizontal zone in a vertical blanking period if the picture signal is an analog signal, or 2-bit additional information is added to picture data if the picture data is digital data.

[0010]

The 2-bit information added by the CGMS system which is referred to hereafter as CGMS information has the following meanings:

[00] --- Copy-free control implementation

[10] --- One-copy control implementation (allowing one-generation copy)

[11] --- Never-copy control implementation (copy strictly prohibited)

The CGMS system does not implement the no-more-copy control implementation described above.

[0011]

If the CGMS information added to picture data is [10], a recording apparatus conforming to the CGMS system will find out that the picture data can be copied and recorded and record a copy of the data. However, the recording apparatus will update the CGMS information to [11] and superpose the updated information on the recorded data. If CGMS information superposed on picture data to be recorded is [11], on the other hand, a recording apparatus conforming to the CGMS system will determine that an operation to copy and record the picture data thereof is prohibited and inhibit a recording operation.

[0012]

[Problems to be Solved by the Invention]

By the way, in a recording apparatus not implementing copy control based on information on copy control such as CGMS information or digital-watermark information, for example, an input main information signal can be copied in some cases even if the input main information signal includes additional information on copy control indicating the never-copy or one-copy control implementation.

[0013]

In order to solve the aforementioned problem, in addition to the digital-watermark and CGMS information described above, information on copyright protection is recorded into a recording medium for recording a main information signal including picture or music data. One can conceive that, by using information on copyright protection, a person committing an illegal copy act can be investigated with ease and can be proven easily, and the use of an illegally copied main information signal can be invalid.

[0014]

Examples of the information on copyright protection are information identifying an author creating the main information signal, various kinds of information useful for proving, investigating or exposure of an illegal copying act and information restricting the use of a main information signal. The information identifying an author includes the name or a code of the author. The information useful for proving, investigating or exposure of an illegal copying act includes a date on which a main information signal is recorded into a recording medium or data for identifying a recording apparatus. The information restricting the use of a main signal includes information indicating a valid period during which the

user is allowed to use the main information signal and the serial number of an apparatus for reproducing the main information signal.

[0015]

In addition, in the case of a disk recording medium, in order to allow a reproducing or recording apparatus to distinguish a read-only ROM disk or a rewritable RAM disk from each other, medium-type identification information is recorded typically in a TOC (Table of Contents) or a directory of the disk. The medium-type identification information is also used as information on copyright protection. For example, by using the medium-type identification information in conjunction with digital-watermark information described above, it is possible to inhibit an operation to reproduce a main information signal obtained as a result of an illegal copy operation.

[0016]

This is because there will be a difference in information on copy control added to a main information signal recorded on a recording medium between an unrewritable read-only ROM disk legally containing a main information signal such as picture data presented by a content maker and a rewritable RAM disk containing information obtained as a result of an operation to copy

a main information signal which is originally recorded on such a ROM disk and presented to the user through communication media such as the Internet.

[0017]

That is to say, in the case of the so-called commercially available ROM disk, digital-watermark information indicating a never-copy control implementation is normally added to a main information signal recorded on the ROM disk in order to protect the disk from an operation to illegally copy the signal.

[0018]

In the case of a RAM disk used by the user mainly for recording a main information signal, on the other hand, digital-watermark information indicating a never-copy or a one-copy control implementation is never added to the main information signal recorded on the disk.

[0019]

That is to say, digital-watermark information which shows a never-copy control implementation and is added to a main information signal recorded on a RAM disk indicates that the main information signal has been obtained as a result of an operation to illegally copy a main information signal recorded on a ROM disk implementing the never-copy control.

[0020]

In addition, when digital-watermark information which shows a one-copy control implementation added to a main information signal recorded on a RAM disk is rewritten by an apparatus implementing copy control based on information on copy control into a no-more-copy control implementation and the main information signal with this digital-watermark information indicating the no-more-copy control implementation is then recorded into the RAM disk. Thus, a main information signal recorded on a RAM disk will not eventually have digital-watermark information indicating a one-copy control implementation. If such a RAM disk exists, the main information signal recorded therein must have been obtained as a result of an illegal copy operation.

[0021]

In addition, even though a main information signal recorded normally on a ROM disk may have additional digital-watermark information indicating a never-copy control implementation, the main information signal is never rewritten into a ROM disk. Thus, there is no way that a main information signal recorded on a ROM disk has additional digital-watermark information indicating a no-more-copy control implementation.

[0022]

It should be noted that additional information indicating a one-copy control implementation for a main information signal recorded on a ROM disk allows a first-generation copy of the main information signal to be produced from the ROM disk. The permission to generate a first-generation copy also means that a copy of the main information signal can always be produced as long as the copy is made from the same ROM disk as an original source and also means that, as a matter of fact, the main information signal can be copied from the ROM disk with a high degree of freedom. The presentation of a main information signal in such a way is not conceived as a desirable presentation from the copyright-protection point of view. Nevertheless, the fact that the use of additional information indicating a one-copy control implementation for a main information signal recorded on a ROM disk is not prohibited means that the presentation of a main information signal in such a way may exist.

[0023]

In order to take advantage of the fact that a difference in information on copy control added to a main control signal recorded on a recording medium exists between a ROM disk and a RAM disk as described above,

there has been conceived a disk reproducing apparatus shown in FIG. 8 wherein control to reproduce a main information signal from a disk such as a DVD is executed by using media identification information of the disk in conjunction with information on copy control such as the digital-watermark information added to the main information signal. The media identification information is also referred to hereafter as information on the media type. The conceivable disk reproducing apparatus of this type is explained as follows.

[0024]

As shown in FIG. 8, an information-signal reproducing apparatus (an information-signal reproducing system) 100 includes a disk reproducing apparatus 101, a data processing unit 102 and a transmission line 103 connecting the disk reproducing apparatus 101 and the data processing unit 102. In this system, the disk reproducing apparatus 101 is implemented typically by a disk drive apparatus for reading out a main information signal from a disk such as a DVD. On the other hand, the data processing unit 102 is a personal computer for carrying out predetermined processing on a main information signal read out by the disk reproducing apparatus 101 from a disk and for outputting a result of

the processing.

[0025]

A disk 300, on which a main information signal to be reproduced has been recorded, is mounted on the disk reproducing apparatus 101. Then, a readout unit 101 reads out the main information signal recorded in a data area of the disk 300 and information on the media type recorded typically in a TOC of the disk 300. The information on the media type is then supplied to a media-type decoding unit 105 employed in the data processing unit 102 through the transmission line 103 and the main information signal is supplied to a digital-watermark-information detecting unit 106 and a switch circuit 108 also employed in the data processing unit 102 through the transmission line 103.

[0026]

The media-type decoding unit 105 decodes the information on the media type, outputting information indicating whether the disk 300 mounted on the disk reproducing apparatus 101 is a RAM or ROM disk to an output control unit 107. On the other hand, the digital-watermark-information detecting unit 106 detects the information on copy control superposed on the main information signal as digital-watermark information,

outputting the information on copy control also to the output control unit 107.

[0027]

The output control unit 107 controls a switch circuit 108 to turn on or off in accordance with the information indicating the media type and the information on copy control. To put it in detail, if the disk 300 is a ROM disk with the information on copy control indicating a no-more-copy control implementation or if the disk 300 is a RAM disk with the information on copy control indicating a never-copy or one-copy control implementation, the output control unit 107 determines that the main information signal recorded on the disk 300 is an illegal copy as described above. In this case, the output control unit 107 executes control to turn off the switch circuit 108, disallowing the main information signal to be supplied to any apparatus at the following stage. Otherwise, the output control unit 107 determines that the main information signal recorded on the disk 300 is legally produced, executing control to turn on the switch circuit 108.

[0028]

In this way, by referring to the information on the media type of a disk containing a recorded main

information signal to be reproduced, the information-signal reproducing system 100 is capable of preventing a main information signal illegally recorded on the disk from being reproduced.

[0029]

If the information on the media type of the disk is improperly altered during transmission between the disk reproducing apparatus 101 and the data processing unit 102, however, a main information signal illegally recorded on the disk can be reproduced and manipulated illegally. As a result, there is raised a problem of repeated illegal copy operations. Assume that a main information signal recorded on a ROM disk with additional digital-watermark information indicating the never-copy control implementation is illegally copied into a RAM disk which normally never includes information on copy control indicating a never-copy control implementation. Since the RAM disk illegally copied the contents of the ROM disk, however, there are some cases where the main information signal copied into the RAM disk has the additional digital-watermark information indicating the never-copy control implementation.

[0030]

In such a case, the information-signal reproducing

system 100 shown in FIG. 8 will not reproduce the main information signal illegally copied into the RAM disk provided that the reproduction control described above is executed normally. With an illegal reproducing system 200 shown in FIG. 9, however, a main information signal obtained as a result of an illegal copy operation can be reproduced and manipulated with a high degree of freedom as described below.

[0031]

A media-type altering apparatus 201 shown in FIG. 9 is used for altering information on the media type read out from a disk by the readout unit 104 employed in the disk reproducing apparatus 101 to information indicating another media type. To be more specific, the media-type altering apparatus 201 alters information on the media type read out from the disk by the readout unit 104 to other media-type information indicating a ROM disk, if the information read out indicates a RAM disk, or to other media-type information indicating a RAM disk if the information indicates a ROM disk. Then, the media-type altering apparatus 201 supplies the altered information on the media type to the media-type decoding unit 105 employed in the data processing unit 102.

[0032]

When a RAM disk is illegally recorded a main information signal with additional digital-watermark information indicating the never-copy control implementation by means of a ROM disk or indicating the never-copy or one-copy control implementation by the way of the Internet, the illegal reproducing system shown in FIG. 9 is capable of normally reproducing a main information signal presented to the user along with additional digital-watermark information indicating the never-copy control implementation or presented to the user along with additional digital-watermark information indicating the never-copy or one-copy control implementation by the way of the Internet. Accordingly, even a main information signal obtained as a result of an illegal copy operation of the signal into a RAM disk can be utilized. In this case, the copyright is infringed by the use of the illegal main information signal.

[0033]

Such infringement of a copyright is made possible by alteration of not only information on the media type but also other information on copyright protection such as information indicating a valid period during which the user is allowed to reproduce a main information and information restricting usable reproducing apparatuses.

That is to say, with these other pieces of information on copyright protection altered after being read out from a disk, control of an operation to reproduce a main information signal can no longer be executed normally. Also in this case, a main information signal obtained as a result of an illegal copy operation or a main information signal with restricted reproduction operations can be reproduced without restrictions and the author of the main information signal loses many benefits, to which the author is entitled.

[0034]

It is thus an object of the present invention addressing the problems described above to provide an apparatus and a method for protecting a copyright of a main information signal with a high degree of reliability and for preventing a main information signal from being copied illegally by substantially disabling an operation to reproduce a main information signal obtained as a result of an illegal copy operation.

[0035]

[Means for Solving the Problems]

In order to solve the problems described above, the present invention and according to claim 1 thereof, there is provided an information-signal reproducing system

including an information-signal reading apparatus for reading out a main information signal and information on copyright protection from a recording medium containing the main information signal and information on at least copyright protection, and an information-signal processing apparatus for receiving the main information signal and the information on copyright protection supplied from the information-signal reading apparatus, wherein the information-signal reading apparatus has: a readout means for reading out the information on copyright protection from the recording medium; an encryption means for encrypting the information on copyright protection read out by the readout means; and an output means for supplying the information on copyright protection encrypted by the encryption means and the unencrypted information on copyright protection to the information-signal processing apparatus, and the information-signal processing apparatus has: a decryption means for decrypting the encrypted information on copyright protection supplied from the information-signal reading apparatus; and a control means for controlling predetermined processing carried out on the main information signal on the basis of the unencrypted information on copyright protection received from the

information-signal reading apparatus and information on copyright protection obtained as a result of decryption carried out by the decryption means.

[0036]

With the information-signal reproducing system according to claim 1, the readout means employed in the information-signal readout apparatus reads out information on copyright protection from a recording medium. By using the information on copyright protection, a person committing an illegal copying act can be investigated with ease, an illegal copying act can also be easily proven and the use of an illegally copied main information signal can be disabled as well.

[0037]

The encryption means encrypts the information on copyright protection read out by the readout means and the output means supplies the information on copyright protection encrypted by the encryption means and the unencrypted information on copyright protection to the information-signal processing apparatus. In this way, both the information on copyright protection encrypted by the encryption means and the unencrypted information on copyright protection are supplied to the information-signal processing apparatus. Even though the contents of

the two pieces of information on copyright protection are the same, the states in which the two pieces of information are transferred to the information-signal processing apparatus are different.

[0038]

In the information-signal processing apparatus, the encrypted information on copyright protection is decrypted by the decryption means. Then, the control means controls predetermined processing carried out on the main information signal on the basis of the unencrypted information on copyright protection supplied from the information-signal reading apparatus and the information on copyright protection obtained as a result of the decryption carried out by the decryption means.

[0039]

As described above, both the information on copyright protection read out from the recording medium and encrypted information on copyright protection are used. Since the encrypted information on copyright protection is difficult to alter, it will be possible to determine whether or not the information on copyright protection has been altered in an attempt to reproduce the main information signal obtained as a result of an illegal copy operation. When thus discriminated being

different from each other, a main information signal obtained as a result of an illegal copy operation can be prevented from being reproduced with a high degree of reliability.

[0040]

In addition, according to claim 2 of the invention, there is provided an information-signal reproducing system as defined in claim 1 above, wherein the information on copyright protection is media-type information indicating the type of the recording medium.

[0041]

With the information-signal reproducing system as set forth in claim 2, the information on the media type recorded in a recording medium is information indicating whether the recording medium is a read-only ROM disk or a writable RAM disk, and is recorded in the TOC or the directory of the recording medium. This information on the media type can be used as information on copyright protection, which is then encrypted and supplied to the information-signal processing apparatus along with the unencrypted one.

[0042]

As described above, it is difficult to alter the encrypted medium-type identification information even

though the unencrypted one read out from the disk can be altered. As a result, if the unencrypted medium-type identification information is found different from the encrypted medium-type identification information, the unencrypted information is determined to have been altered in an attempt to reproduce a main information signal resulting from an illegal copy operation. Thus, a main information signal obtained as a result of an illegal copy operation can be prevented from being reproduced with a high degree of reliability.

[0043]

In addition, according to claim 3 of the invention, there is provided an information-signal reproducing system as defined in claim 1 above, wherein the encryption means employed in the information-signal reading apparatus encrypts the information on copyright protection in accordance with a CSS system.

[0044]

With the information-signal reproducing system as set forth in claim 3, the information on copyright protection read out by the information-signal readout means are subjected to the encryption processing according to the CSS (Contents Scramble System), similar to the encryption processing subjected to such as image

data recorded on a disk like DVD, by the encryption means provided in the information-signal reading system.

[0045]

As described above, it is difficult to alter the encrypted information on copyright protection, thereby the information on copyright protection is securely supplied from the information-signal reading system to the information-signal processing apparatus. Thus, a main information signal obtained as a result of an illegal copy operation can be prevented from being reproduced with a high degree of reliability, on the basis of the information on copyright protection and the encrypted information on copyright protection.

[0046]

In addition, according to claim 4 of the invention, there is provided an information-signal reproducing system as defined in claim 1 above, wherein additional information for controlling a copy operation has been added to the main information signal recorded on the recording medium; the information-signal processing apparatus is provided with an additional-information detecting means for detecting the additional information added to the main information signal received from the information-signal reading apparatus; and the control

means controls predetermined processing carried out on the main information signal by taking the additional information detected by the information-signal detecting means into consideration.

[0047]

With the information-signal reproducing system as set forth in claim 4, the main information signal read out from a recording medium includes an additional information for operating copy control of the main information signal. The additional information indicates the content, for example, "Copy Free", "One Copy", "No More Copy", "Never Copy" and so on.

[0048]

The main information signal is read out by the information-signal readout means, so that supplied to the information-signal processing apparatus. In the information-signal processing apparatus, the additional information added to the main information signal by the additional-information detecting means is detected. In consideration of the detected additional information, the control means executes control of predetermined processing carried out on the main information signal by the information-signal readout means.

[0049]

As described above, whether or not the information signal recorded on the recording medium is illegally copied is reliably determined, with consideration given to the additional information for controlling the copy operation added to the main information signal. Thereby the reproduction control of the information signal recorded on the recording medium is executed appropriately and reliably.

[0050]

In addition, according to claim 5 of the invention, there is provided an information-signal reproducing system as defined in claim 4, wherein the additional information is information superposed on the main information signal as digital-watermark information; and the additional-information detecting means employed in the information-signal processing apparatus detects the digital-watermark information superposed on the main information signal.

[0051]

With the information-signal reproducing system as set forth in claim 5, the additional information for controlling a copy operation is superposed on the main information signal as digital-watermark information, thereby it is difficult to delete or alter the additional

information itself. However, the additional-information detecting means employed in the information-signal processing apparatus detects the digital-watermark information reliably.

[0052]

As described above, the additional information for controlling a copy operation added as digital-watermark information on the main information signal is detected. In consideration of the additional information, the reproduction control of the main information signal can be executed more appropriately and reliably.

[0053]

In addition, according to claim 6 of the invention, there is provided an information-signal reproducing system, including an information-signal reading apparatus for reading out a main information signal and information on copyright protection from a recording medium containing the main information signal and information on at least copyright protection, and an information-signal processing apparatus for receiving the main information signal and the information on copyright protection received from the information-signal reading apparatus, wherein the information-signal reading apparatus has: readout means for reading out the information on

copyright protection from the recording medium;
encryption means for encrypting the information on
copyright protection read out by the readout means;
output means for supplying the information on copyright
protection encrypted by the encryption means and the
unencrypted information on copyright protection to the
information-signal processing apparatus; and readout
control means for controlling an operation to read out
the main information signal from the recording medium in
accordance with a readout-control signal received from
the information-signal processing apparatus, and the
information-signal processing apparatus has: decryption
means for decrypting the encrypted information on
copyright protection received from the information-signal
reading apparatus; and readout-control-signal generating
means for generating the readout-control signal based on
the unencrypted information on copyright protection
received from the information-signal reading apparatus
and information on copyright protection obtained as a
result of decryption carried out by the decryption means
and for supplying the readout-control signal to the
information-signal reading apparatus.

[0054]

With the information-signal reproducing system as

set forth in claim 6, the system includes information-signal reading apparatus in which, information on copyright protection is read out by the readout means from a recording medium and supplied to the encryption means. Then, the encrypted information on copyright protection is supplied to the information-signal processing apparatus along with the unencrypted information on copyright protection.

[0055]

In the information-signal processing apparatus, the information on copyright protection encrypted by the encryption means is decrypted by the decryption means. Then, the readout-control-signal generating means generates the readout-control signal based on the unencrypted information on copyright protection received from the information-signal reading apparatus and the information on copyright protection decrypted by the decryption means, and supplies the generated readout-control signal to the information-signal reading apparatus.

[0056]

In the information-signal reading apparatus, the readout control means controls an operation to read out the main information signal from the recording medium on

the basis of the readout-control signal received from the information-signal processing apparatus.

[0057]

As described above, reproduction of illegally copied information signal by altering information on copyright protection can be prevented reliably. In this case, an operation itself to read out the main information signal from the recording medium is controlled, so that the reproduction of the main information signal is controlled reliably.

[0058]

In addition, according to claim 7 of the invention, there is provided the information-signal reproducing system as defined in claim 6 above, wherein the information-signal processing apparatus is provided with a readout-control-signal encrypting means for encrypting a readout-control signal generated by the readout-control-signal generating means; and the information-signal reading apparatus is provided with control-information decrypting means for receiving and decrypting encrypted a readout-control signal received from the information-signal processing apparatus.

[0059]

With the information-signal reproducing system

according to claim 7, the readout-control signal encrypted by the readout-control-signal encrypting means of the information-signal processing apparatus is supplied to the information-signal reading apparatus. The encrypted readout-control signal is decrypted by the control-information decrypting means of the information-signal reading apparatus. On the basis of the decrypted readout-control signal, the readout control means operates controlling for reading out the main information signal from a recording medium.

[0060]

As described above, for example, in an attempt to reproduce the main information signal obtained as a result of an illegal copy operation, both the encrypted information on copyright protection read out from the information-signal reading apparatus and the encrypted readout-control-signal supplied from the information-signal processing apparatus need to be altered. However, since both of them are encrypted, it is difficult to alter them. Thus, the reliability for the information-signal reproducing system is further enhanced.

[0061]

In addition, according to claim 8 of the invention, there is provided an information-signal reproducing

system as defined in claim 6 above, wherein the information on copyright protection is media-type information indicating the type of the recording medium.

[0062]

With the information-signal reproducing system as set forth in claim 8, the information-signal processing apparatus is supplied with the both of unencrypted and encrypted media-type information indicating ROM disk or RAM disk, as information on copyright protection.

[0063]

As described above, even if the unencrypted media-type information is altered, it is difficult to alter the encrypted media-type information. If the unencrypted information on the media type is different from the encrypted information on the media type, media-type information is determined to have been altered for reproduction of illegal-copied information-signal, so that information-signal reproducing apparatus can operate controlling for reading out the information signal appropriately and reliably.

[0064]

In addition, according to claim 9 of the invention, there is provided an information-signal reproducing system as defined in claim 6 above, wherein the

encryption means employed in the information-signal reading apparatus encrypts the information on copyright protection in accordance with a CSS system.

[0065]

With the information-signal reproducing system as set forth in claim 9, when a main information signal recorded on a disk recording medium such as DVD is provided to the information-signal processing apparatus, the information on copyright protection is also, similar to a main information, subjected to the encryption processing according to the CSS system, then supplied to the information-signal processing apparatus.

[0066]

As described above, since the information on copyright protection can not be altered easily, the encrypted information on copyright protection is surely supplied from the information-signal reading apparatus to the information-signal processing apparatus. Then, in accordance with the information on copyright protection and encrypted information on copyright protection, the information-signal reading apparatus operates readout process of the main information signal, appropriately and reliably.

[0067]

In addition, according to claim 10 of the invention, there is provided an information-signal reproducing system as defined in claim 7 above, wherein the readout-control-signal encrypting means employed in the information-signal processing apparatus carries out encryption processing in accordance with a system different from a system for the encryption means employed in the information-signal reading apparatus.

[0068]

With the information-signal reproducing system as set forth in claim 10, the information on copyright protection is encrypted in accordance with a system which is different from a system for encrypting the readout-control signal. As described above, if the illegal copied information-signal on a recording medium is to be reproduced, both the encrypted information on copyright protection and the readout-control signal are needed to be decrypted. Thus, the reliability for the information-signal reproducing system is enhanced.

[0069]

In addition, according to claim 11 of the invention, there is provided the information-signal reproducing system as defined in claim 6 above, wherein: additional information for controlling a copy operation has been

added to the main information signal recorded on the recording medium; the information-signal processing apparatus is provided with additional-information detecting means for detecting the additional information added to the main information signal received from the information-signal reading apparatus; and the readout-control-signal generating means generates a readout-control signal to be supplied to the information-signal reading apparatus by taking the additional information detected by the additional-information detecting means into consideration.

[0070]

With the information-signal reproducing system as set forth in claim 11, the main information signal read out from a recording medium includes an additional information for operating copy control of the main information signal. The additional information indicates the content, for example, "Copy Free", "One Copy", "No More Copy", "Never Copy" and so on.

[0071]

In the information-signal processing apparatus, the additional information added to the main information signal is detected by the additional-information detecting means. By taking the detected additional

information into consideration, the readout-control signal is generated by the readout-control-signal generating means, and supplied to the information-signal reading apparatus.

[0072]

As described above, in accordance with the information on copyright protection and the additional information for copy control added to the main information signal, the information-signal reading apparatus operates controlling for readout process of information signal, appropriately and reliably.

[0073]

In addition, according to claim 12 of the invention, there is provided an information-signal reproducing system as defined in claim 11 above, wherein: the additional information is information superposed on the main information signal as digital-watermark information; and the additional-information detecting means employed in the information-signal processing apparatus detects the digital-watermark information superposed on the main information signal.

[0074]

With the information-signal reproducing system as set forth in claim 12, the additional information for

copy control is superposed on the main information as digital-watermark information, so that it is difficult to delete or alter the additional information itself.

However, the additional-information detecting means of the information-signal processing apparatus surely detects the digital-watermark.

[0075]

As described above, in accordance with the information on copyright protection and the additional information provided as digital-watermark information added to the main information, the information-signal reading apparatus operates controlling for readout process of information signal, appropriately and reliably.

[0076]

[Mode for Carrying out the Invention]

Next, an information-signal reproducing system, an information-signal reading apparatus, an information-signal processing apparatus, an information-signal reproducing method, an information-signal reading method and an information-signal processing method as implemented by embodiments of the present invention are described by referring to diagrams.

[0077]

(Overview of the Information-Signal Reproducing System)

First of all, an overview of the information-signal reproducing system (information-signal reproducing apparatus) implemented by an embodiment of the present invention is described. The information-signal reproducing system implemented by the embodiment described below includes an information-signal reading apparatus for reading out a main information signal from a recording medium and an information-signal processing apparatus for carrying out predetermined processing on the main information signal read out by the information-signal reading apparatus.

[0078]

In an operation to reproduce data such as a main information signal like picture information from a disk recording medium, the information-signal reproducing system also forms a determination as to whether or not the main information signal to be reproduced has been obtained as a result of an illegal copy operation in order to prevent an illegal main information signal from being reproduced. As a result, the copyright on the main information signal can be protected and an illegal operation to copy the main information signal can be avoided.

[0079]

The formation of a determination as to whether or not a main information signal recorded on a disk recording medium has been obtained as a result of an illegal copy operation is based on information on copyright protection recorded on the disk recording medium along with the main information signal to be reproduced and based on digital-watermark information used as information on copy control added to the main information signal for implementing copy control.

[0080]

As described above, information on copyright protection is various kinds of information recorded on a recording medium so as to allow a person committing an illegal copying act to be investigated with ease and to be also proven easily, and the use of an illegally copied main information signal to be disabled as well. In the embodiments described below, the information on copyright protection is exemplified by adapting information on the media type having a predetermined relation with the information on copy control.

[0081]

A disk recording medium can be either an unrewritable read-only ROM disk containing a main information signal recorded legally by a content maker,

or a RAM disk recorded with information which can be rewritten by the user. These two types of disk can be distinguished from each other by detecting information on the media type recorded in the TOC or the directory of each disk.

[0082]

The information on copy control added to a main information signal recorded on a ROM disk presented to the user to protect a copyright can be copy-free control information which is an exception allowing unrestricted copy operations, or never-copy control information absolutely prohibiting production of a copy as described earlier.

[0083]

In the case of a main information signal presented to the user by way of the Internet or through broadcasting media, it is possible to add information on copy control indicating a never-copy control implementation absolutely prohibiting production of a copy, or a one-copy control implementation allowing only the first-generation copy to be produced. In the case of a RAM disk, no-more-copy control information shall be added to a main information signal recorded on the disk to indicate that no more copies of the signal can be

produced.

[0084]

Thus, any pair of information on the media type and information on copy control added to a main information signal other than those described above is determined to indicate that the main information signal has been obtained as a result of an illegal copy operation and its use can be restricted. In addition, the information-signal reproducing system described below is also capable of preventing a main information signal obtained as a result of an illegal copy operation from being reproduced and utilized by alteration of the information on the media type.

[0085]

It should be noted that the disk recording medium used in the embodiment described below is a DVD. In addition, while various kinds of data such as a video signal (or picture data), an audio signal and a program can be recorded as a main information signal on the DVD, it is assumed in the following description that the main information signal recorded on the DVD is a video signal in order to make the description simple. In the following description, a rewritable DVD is referred to as a RAM disk while an unrewritable read-only DVD is referred to

as a ROM disk.

[0086]

(Presentation of an Information Signal to the User)

The following description includes an explanation of presentation of a digital video signal with information on copy control added thereto. Routes through which an information signal is presented to the user include a ROM disk produced by a content maker, a network such as the Internet and broadcasting media such as satellite broadcasting or cable broadcasting.

[0087]

In either case, since the digital video signal may be illegally copied and used, information on copy control is added to the digital video signal as digital-watermark information which is difficult to alter, and the digital video signal is subjected typically to encryption processing (scramble processing) according to the CSS system.

[0088]

It should be noted that, in the embodiments, the information on copy control is subjected to a spectrum-spreading process by using a series of PN (Pseudo-random Noise) codes which are referred to hereafter as PN codes, and the information on copy control completing the

spectrum-spreading process is superposed on the digital video signal as digital-watermark information.

[0089]

First of all, presentation of a main information signal by means of a ROM disk is explained by referring to FIG. 6. FIG. 6 is a block diagram showing a recording apparatus used by a content maker to record a main information signal in a process to produce a regular ROM disk wherein a recorded digital video signal and digital-watermark information added thereto as information on copy control are subjected to the encryption processing according to the CSS system before being recorded onto the ROM disk.

[0090]

As shown in FIG. 6, a digital video signal S51 to be recorded onto a ROM disk 400 is supplied to an adder 53 by way of an input terminal 51. Meanwhile, from an input terminal 52, a vertical synchronization signal VD separated from the digital video signal S51 is supplied as a timing signal to a PN-code generating unit 541 and an information on copy control generating unit 542 which are employed in an SS (spectrum spreading)-information on copy control generating unit 54.

[0091]

Using a clock signal synchronized with the vertical synchronization signal VD, the PN-code generating unit 541 generates a series of PN codes starting with the first code to be used in a spectrum-spreading process of the information on copy control by each N fields, where N is an integer.

[0092]

At the same time, using the clock signal synchronized with the vertical synchronization signal VD, the information on copy control generating unit 542 generates an information on copy control series to be superposed on the digital video signal by each N fields in the same way as the PN-code generating unit 541. The series of PN codes generated by the PN-code generating unit 541 and the information on copy control series generated by the information on copy control generating unit 542 are supplied to a multiplier 543.

[0093]

That is to say, the PN-code generating unit 541 and the information on copy control generating unit 542 generate a series of PN codes and the information on copy control series, respectively starting from the beginnings of the series by using the same clock signals with the same timing synchronized to the vertical synchronization

signal VD by typically each field or by each frame, supplying the series of the codes and the information to the multiplier 543.

[0094]

In the multiplier 543, the information on copy control series is subjected to a spectrum-spreading process by using the series of PN codes to generate SS-information on copy control which is then supplied to a level control unit 544. The level control unit 544 adjusts the level of the SS-information on copy control so that the SS-information on copy control has such a low level as not to disturb a picture represented by the digital video signal when the picture is displayed on a monitor to which the digital video signal is supplied along with the SS-information on copy control superposed thereon. The SS-information on copy control S52 with an adjusted level is then supplied to the adder 53.

[0095]

The adder 53 superposes the SS-information on copy control S52 on the digital video signal S51 to generate a digital video signal S53. The digital video signal S53 with the SS-information on copy control S52 superposed thereon is then supplied to a data compressing unit 55. The data compressing unit 55 compresses the digital video

signal S53 in accordance with the MPEG system, supplying a compressed digital video signal S54 to an encryption unit 56.

[0096]

In this embodiment, the encryption unit 56 carries out encryption processing according to the CSS system on the digital video signal S54, if the information on copy control superposed on the digital video signal S54 prohibits copy operation or restricts production of copy generations, to generate an encrypted digital video signal S55 which is then supplied to a write unit 58.

[0097]

The write unit 58 also receives information on the media type from a media-type generating unit 57. As described above, the information on the media type indicates whether the disk 400 is a ROM or RAM disk. The write unit 58 writes the information on the media type into an area in the disk 400, such as the TOC or the directory, into which the user never records data. In this case, since the disk 400 is a ROM disk, the information on the media type indicating that the disk 400 is a ROM disk is recorded into the disk 400.

[0098]

In addition, as for the encrypted digital video

signal S25, the write unit 58 also records information such as an encryption key used in the processing to encrypt the digital video signal S25 in accordance with the CSS system into an area on the disk 400 from which the user can not read out data. The digital video signal S55 itself is also written by the write unit 58 into the data area of the disk 400.

[0099]

In this way, it is possible to produce the so-called "commercially available" ROM disk containing a digital video signal with SS-information on copy control superposed thereon as digital-watermark information or containing a digital video signal completing encryption processing according to the CSS system in order to implement copy generation restriction on the digital video signal.

[0100]

As described earlier, the information on copy control indicates one of the control implementations, namely, copy free, one copy (allowing the first copy generation to be produced), no more copy (allowing no subsequent copy generations to be produced) and never copy (absolutely allowing no copy).

[0101]

The disk 400 is the ROM disk produced legitimately by a content maker to contain a digital video signal. The never-copy control information is superposed on the digital video signal recorded into the disk 400 to protect the digital video signal against an illegal copy operation.

[0102]

Subjected to a spectrum-spreading process and superposed on the digital video signal as digital-watermark information, the information on copy control does not degrade the digital video signal, and can not be removed or altered. The information on copy control superposed on the digital video signal as digital-watermark information can be detected by equipment to be described later such as a data processing unit or a recording apparatus with a high degree of reliability, making it possible to execute control of processing carried out on the information signal such as reproduction control and copy control based on the detected information on copy control.

[0103]

FIGS. 7A to 7D are diagrams showing relations between the SS-information on copy control superposed on the digital video signal and the digital video signal in

terms of a spectrum. The information on copy control is a signal that conveys a small amount of information having a low bit rate and occupies a narrow band as shown in FIG. 7A. After completing the spectrum-spreading process, the information on copy control becomes a signal occupying a broad band as shown in FIG. 7B. As shown in FIGS. 7A and 7B, the level of the SS-information on copy control (the spectrum-spreading processed signal) is inversely proportional to the width of the band.

[0104]

As described above, the SS-information on copy control is added to the digital video signal S51 by the adder 53. The adder 53 superposes the SS-information on copy control on the digital video signal S51 at a level smaller than a dynamic range of the digital video signal S51 as shown in FIG. 7C, so that the digital video signal S51 is hardly degraded by the superposition. Thus, when the digital video signal with SS-information on copy control superposed thereon is reproduced and supplied to a monitor receiver to display pictures thereon, effects of the SS-information on copy control hardly exist. As a result, fine reproduced pictures can be obtained.

[0105]

As will be described later, if a spectrum-inverse-

spreading process needs to be carried out in order to detect the SS-information on copy control, the SS-information on copy control is restored back into a signal with a narrow band as shown in FIG. 7D as a result of the spectrum-inverse-spreading process. By providing a sufficiently large band spreading factor, the power of information on copy control detected as a result of the spectrum-inverse-spreading process is greater than the information signal which is the video signal in the case of the embodiment, thereby being detected.

[0106]

In this case, since the SS information on copy control added to the video signal is superposed thereon at the same time and at the same frequency as the video signal, the SS information on copy control can be removed and corrected by using a frequency filter and a simple information replacement technique respectively.

[0107]

Thus, by superposing necessary SS information on copy control on a video signal and recording the signal, the information on copy control can be transferred to a receiver with a high degree of reliability. In addition, if the information on copy control to be superposed on an information signal such as a video signal is subjected to

a spectrum-spreading process at a signal power smaller than that of the information signal as is the case with the above-mentioned embodiment, degradation of the information signal can be minimized.

[0108]

Therefore, since it is thus hard to alter and remove SS information on copy control superposed on an information signal such as a video signal, an operation to illegally copy a video signal can be made difficult.

[0109]

As already mentioned, information on the media type is recorded on a disk 400 for recording a digital video signal by using the recording apparatus 50 shown in FIG. 6. It should be noted, however, that by manufacturing a disk containing information on the media type from the beginning, it is not necessary to the record information on the media type on the disk for recording a main-information signal such as a digital video signal by using the recording apparatus.

[0110]

In addition, when a digital video signal to include the never-copy or one-copy control information described above is presented to the user by way of the Internet or by means of broadcasting media, for example, the

information on copy control is superposed on the digital video signal as digital-watermark information and the digital video signal including the information on copy control are subsequently compressed in accordance with the MPEG system and then encrypted in accordance with the CSS system in the same way as the recording apparatus 50 shown in FIG. 6 before being presented to the user.

[0111]

A digital video signal presented to the user by means of a regularly produced ROM disk or through the Internet or broadcasting media as described above may be copied illegally into a RAM disk. An information-signal reproducing system to be described next is capable of preventing the digital video signal recorded on such a RAM disk from being reproduced for illegal use by alteration of the information on the media type explained earlier with reference to FIG. 9. That is to say, by disabling an operation to reproduce a digital video signal illegally copied into a recording medium such as a RAM disk, it is possible to protect the copyright on the digital video signal and, hence, to prevent an information signal from being illegally copied.

[0112]

(First Embodiment)

FIG. 1 is a block diagram used for explaining an information-signal reproducing system (information-signal reproducing apparatus) 10 implemented by a first embodiment. As shown in the figure, the information-signal reproducing system 10 includes a disk reproducing apparatus 11 and a data processing unit 12 which are connected to each other by a transmission line (bus) 13 for exchanging information signals.

[0113]

As shown in FIG. 1, the disk reproducing apparatus 11 includes a readout unit 111 and a media-type encrypting unit 112. On the other hand, the data processing unit 12 includes a media-type decoding unit 121, a decryption unit 122, an MPEG decoding unit 123, a digital-watermark-information detecting unit 124, an output control unit 125, and a switch circuit 126.

[0114]

The readout unit 111 employed in the disk reproducing apparatus 11 reads out information on the media type T_j and a digital video signal V_i from a disk DK mounted on the disk reproducing apparatus 11. As described above, this digital video signal V_i is obtained as a result of a series of processes wherein the information on copy control is superposed on an original

digital video signal as digital-watermark information and the digital video signal Vi including the information on copy control are subsequently compressed in accordance with the MPEG system and then encrypted in accordance with the CSS system. Both the information on the media type Tj and the digital video signal Vi thus read out are then supplied to the data processing unit 12 through the transmission line 13.

[0115]

In addition, the information on the media type Tj read out by the readout unit 111 is supplied to the media-type encrypting unit 112 also employed in the disk reproducing apparatus 11. In this embodiment, the information on the media type Tj is encrypted in accordance with the CSS system, being converted into encrypted information on the media type STj. Then, the encrypted information on the media type STj is also supplied to the data processing unit 12 through the transmission line 13.

[0116]

In the data processing unit 12, the encrypted information on the media type STj and the digital video signal Vi are supplied to the decryption unit 122 whereas the information on the media type Tj is supplied to the

media-type decoding unit 121 as shown in FIG. 1.

[0117]

The decryption unit 122 decrypts the encrypted digital video signal V_i and the encrypted information on the media type ST_j by using an algorithm for the encryption carried out on the digital video signal V_i and the information on the media type ST_j or a correct encryption key to produce a decrypted digital video signal V_m and decrypted information on the media type M_t . A correct decrypted digital video signal V_m and correct decrypted information on the media type M_t are obtained only if a correct algorithm or a correct encryption key is used, that is, only if the decryption is carried out correctly.

[0118]

If the decryption can not be carried out normally, the switch circuit 126 is turned off by the output control unit 125 so as not to output the video signal.

[0119]

The digital video signal V_m normally decrypted by the decryption unit 122 is supplied to the MPEG decoding unit 123 and the information on the media type M_t normally decrypted by the decryption unit 122 is supplied to the media-type decoding unit 121.

[0120]

The MPEG decoding unit 123 decompresses the digital video signal Vm which has been compressed in accordance with the MPEG system to restore the original digital video signal V. The restored original digital video signal V is supplied to the digital-watermark-information detecting unit 124 and an input terminal of the switch circuit 126.

[0121]

The digital-watermark-information detecting unit 124 detects the information on copy control which is the digital-watermark information superposed on the supplied digital video signal. As described above, the digital-watermark information superposed on the digital video signal has completed a spectrum-spreading process. The digital-watermark-information detecting unit 124 detects the information on copy control by carrying out a spectrum-inverse-spreading process.

[0122]

In the first embodiment, the digital-watermark-information detecting unit 124 employed in the data processing unit 12 includes a multiplier 241, a synchronization detector 242, a PN-code generator 243 and a code identifier 244 as shown in FIG. 2. The digital

video signal V from the MPEG decoding unit 123 is supplied to the multiplier 241 and the synchronization detector 242 employed in the digital-watermark-information detecting unit 124. The synchronization detector 242 detects a vertical synchronization signal VD from the digital video signal V, supplying the vertical synchronization signal VD to the PN-code generator 243.

[0123]

The PN-code generator 243 generates a series of PN codes by using a clock signal synchronized to the vertical synchronization signal VD with each PN code generated with timing synchronized to the vertical synchronization signal VD in the same way as the generation of the series of PN codes used in the spectrum-spreading process in the recording circuit 50 shown in FIG. 6. That is to say, the series of PN codes is generated with the same timing as that used in the spectrum-spreading process of the digital-watermark information superposed on the digital video signal and supplied to the multiplier 241.

[0124]

The multiplier 241 carries out a spectrum-inverse-spreading process by multiplying the digital video signal V by the series of PN codes received from the PN-code

generator 243 in order to detect a copy-control-information series superposed on the digital video signal V, supplying the copy-control-information series to the code identifier 244.

[0125]

The code identifier 244 determines the contents of the information on copy control from the supplied copy-control-information series, supplying the result to the output control unit 125. To put in detail, from the copy-control-information series obtained from the spectrum-inverse-spreading process, the code identifier 244 detects whether the information on copy control superposed on the digital video signal V is the copy-free control information allowing copy operations to be carried out freely, the one-copy control information allowing only the first-generation copy to be produced, the no-more-copy control information allowing no further generation copies or the never-copy control information absolutely prohibiting copy operations. The detected type of the information on copy control is supplied to the output control unit 125.

[0126]

In the mean time, the media-type decoding unit 121 decodes the information on the media type Tj received

from the disk reproducing apparatus 11 and the decrypted information on the media type Mt received from the decryption unit 122 to detect information indicating whether the disk DK mounted on the disk reproducing apparatus 11 is a ROM or RAM disk, supplying the detected information on the disk type to the output control unit 125. At that time, if the information on the media type Tj is different from the decrypted information on the media type Mt or one of them is missing, the information on the media type is determined to have been altered. In this case, a request to inhibit a reproduction operation is output to the output control unit 125.

[0127]

Receiving the request to inhibit a reproduction operation, the output control unit 125 turns off the switch circuit 126 so that the digital video signal V completing the MPEG decoding process in the MPEG decoding unit 123 is not output. If information on the media type is received from the media-type decoding unit 121 instead of the request to inhibit a reproduction operation, on the other hand, the output control unit 125 turns the switch circuit 126 on or off based on the information on the media type received from the media-type detecting unit 121 and the information on copy control detected by

the digital-watermark-information detecting unit 124.

[0128]

To be more specific, if the information on the media type received from the media-type decoding unit 121 indicates that the disk DK is a ROM disk and the information on copy control received from the digital-watermark-information detecting unit 124 is the never-copy control information, the switch circuit 126 is turned on to allow the MPEG decoding unit 123 to output the digital video signal V completing the MPEG decoding process.

[0129]

It should be noted that, in another case which is hardly possible from the copyright-protection point of view as described earlier, the one-copy control information allowing the first-generation copy to be produced is added to a video signal recorded on a ROM disk. Also for such a disk, the switch circuit 126 is turned on to allow the MPEG decoding unit 123 to output the digital video signal V completing the MPEG decoding process.

[0130]

If the information on the media type received from the media-type decoding unit 121 indicates that the disk

DK is a ROM disk and the information on copy control received from the digital-watermark-information detecting unit 124 is the no-more-copy control information, the switch circuit 126 is turned off to prevent the digital video signal V completing the MPEG decoding process from being output.

[0131]

If the information on the media type received from the media-type decoding unit 121 indicates that the disk DK is a RAM disk and the information on copy control received from the digital-watermark-information detecting unit 124 is the no-more-copy control information, the switch circuit 126 is turned on to allow the MPEG decoding unit 123 to output the digital video signal V completing the MPEG decoding process.

[0132]

If the information on the media type received from the media-type decoding unit 121 indicates that the disk DK is a RAM disk and the information on copy control received from the digital-watermark-information detecting unit 124 is the never-copy or one-copy control information, the switch circuit 126 is turned off to prevent the digital video signal V completing the MPEG decoding process from being output. It should be noted

that such a RAM disk with such information on copy control is not seen in the normal usage as described before.

[0133]

As described above, the encrypted information on the media type STj is output by the disk reproducing apparatus 11 to the data processing unit 12 along with the digital video signal Vi and the information on the media type Tj. Since the encrypted information on the media type STj is obtained as a result of an encryption process, it is not easy to alter the information STj. Thus, by merely altering the information on the media type Tj, an operation to reproduce the digital video signal Vi can not be carried out since a result of comparison of the encrypted information on the media type STj with the information on the media type Tj will immediately indicate whether or not the information on the media type Tj has been altered.

[0134]

Assume that a digital video signal with the never-copy control information superposed thereon is illegally copied from a ROM disk (which is the legal means of presentation of the digital video signal) to a RAM disk, and the information on the media type is changed from

information indicating a RAM disk to one indicating a ROM disk. Even in this case, an operation to reproduce the illegally copied digital video signal is disabled.

[0135]

Assume that a digital video signal on which digital-watermark information such as the never-copy or one-copy control information presented to the user through the Internet or broadcasting media and illegally copied to a RAM disk is superposed, and that the information on the media type is changed from information indicating a RAM disk to one indicating a ROM disk in an operation to reproduce the illegally copied digital video signal. In this case, similarly, such an illegal operation is also disabled as well.

[0136]

As described above, it is possible to reliably prevent a digital video signal obtained as a result of an illegal copy operation from being utilized. In addition, even when the information on the media type Tj is not altered, it is also possible to prevent a digital video signal obtained as a result of an illegal copy operation from being reproduced on the basis of the information on the media type and the information on copy control detected from the digital video signal. As added to the

digital video signal as digital-watermark information, the information on copy control can not be removed and altered. Thus, it is possible to reliably execute control of an operation to reproduce the digital video signal in consideration of the information on copy control.

[0137]

(Modification of the First Embodiment)

In the first embodiment described earlier, a digital video signal presented to the user by using a ROM disk or through a network such as the Internet is obtained by superposing information on copy control on a base-band digital video signal prior to an MPEG encoding process in digital-watermark processing as described earlier with reference to FIG. 6.

[0138]

However, information on copy control may be superposed in digital-watermark processing on an elementary stream obtained as a result of an MPEG encoding process of the digital video signal. In this case, the information on copy control superposed on the digital video signal as digital-watermark information can be detected from the digital video signal completing the MPEG encoding process.

[0139]

For such a case, an information-signal reproducing system shown in FIG. 3 can be constructed. A watermark-information detecting unit 211 employed in a data processing unit 21 of the information-signal reproducing system is different from the watermark-information detecting unit 124 shown in FIG. 1. However, the other components are identical with their counterparts shown in FIG. 1. Components in FIG. 3 identical with their counterparts shown in FIG. 1 are denoted by the same reference numerals as the latter and their explanation is not repeated.

[0140]

The watermark-information detecting unit 211 employed in a data processing unit 21 detects information on copy control superposed on the MPEG encoded digital video signal Vm as digital-watermark information prior to the MPEG decoding process. To be more specific, the watermark-information detecting unit 211 detects whether the information on copy control superposed on the digital video signal Vm prior to the MPEG decoding process is the copy-free control information, the one-copy control information allowing first-generation copies to be produced, the no-more-copy control information or the never-copy control information, and supplies the detected

type of the information on copy control to the output control unit 125.

[0141]

As described above, even in the case of information on copy control superposed in digital-watermark processing on an elementary stream obtained as a result of an MPEG encoding process of the digital video signal, it is possible to reliably execute control of an operation to reproduce the digital video signal based on the information on the media type Tj and the information on copy control STj. To put it in detail, an operation to reproduce a digital video signal from the disk DK can be controlled correctly and reliably on the basis of the information on the media type Tj output by the media-type decoding unit 121 and the information on copy control detected by the digital-watermark-information detecting unit 211.

[0142]

As shown in FIG. 3, the MPEG decoding unit 123 is placed between the decryption unit 122 and the switch circuit 126. It should be noted, however, that the MPEG decoding unit 123 can also be provided after the switch circuit 126. In this case, the MPEG compressed digital video signal is supplied to the MPEG decoding unit 123

only if the switch circuit 126 is turned on by the output control unit 125, that is, only if an operation to reproduce the digital video signal is allowed.

[0143]

Thus, in this case, only a digital video signal, the reproduction operation of which is allowed, is subjected to an MPEG decoding process. A video signal obtained as a result of an illegal copy operation or a video signal accompanied by information on the media type altered during the transmission between the disk reproducing apparatus and the data processing unit is not subjected to the MPEG decoding process.

[0144]

(Second Embodiment)

In the information-signal reproducing system implemented by the first embodiment described above, the operation to output a video signal from the data processing unit 12 or 21 is controlled on the basis of unencrypted information on the media type, encrypted information on the media type and information on copy control superposed on the video signal as digital-watermark information.

[0145]

As a result, even if the outcome of a determination

based on the unencrypted information on the media type, the encrypted information on the media type and the information on copy control superposed on the digital video signal as digital-watermark information indicates that the video signal is obtained as a result of an illegal copy operation, the operation to read out the digital video signal from the disk and the operation to transmit the digital video signal along with the pieces of information on the media type and information on copy control from the disk reproducing apparatus 11 to the data processing unit 12 or 21 are continued.

[0146]

In the case of the information-signal reproducing system implemented by the second embodiment, on the other hand, if the digital video signal to be reproduced and used is determined to have been obtained as a result of an illegal copy operation, or the unencrypted information on the media type or the encrypted information on the media type supplied by the disk reproducing apparatus to the data processing unit is determined to have been altered, the operation to read out the digital video signal from the disk itself is disabled so that the signal can not be reproduced.

[0147]

FIG. 4 is a block diagram showing an information-signal reproducing system 30 implemented by the second embodiment. Much like the information-signal reproducing system 10 implemented by the first embodiment shown in FIG. 1, the information-signal reproducing system 30 implemented by the second embodiment includes a disk reproducing apparatus 31 and a data processing unit 32 which are connected to each other by a transmission line (bus) 33 for exchanging information signals.

[0148]

As shown in FIG. 4, the disk reproducing apparatus 31 includes a readout unit 311, a media-type encrypting unit 312, a control-signal decrypting unit 313 and readout control unit 314. On the other hand, the data processing unit 32 includes a media-type decoding unit 321, a decryption unit 322, an MPEG decoding unit 323, a digital-watermark-information detecting unit 324, a control-signal generating unit 325 and a control-signal encrypting unit 326.

[0149]

The readout unit 311 and the media-type encrypting unit 312 employed in the disk reproducing apparatus 31 as well as the media-type decoding unit 321, the decryption unit 322, the MPEG decoding unit 323 and the digital-

watermark-information detecting unit 324 employed in the data processing unit 32 are identical with their respective counterparts in the disk reproducing apparatus 11 and the data processing unit 12 of the first embodiment described earlier.

[0150]

Much like the first embodiment, information on the media type is recorded on the TOC or the directory of the disk DK mounted on the disk reproducing apparatus 32. In addition, a digital video signal and information on copy control superposed thereon are recorded in a data area of the disk DK. As described above, the digital video signal and the information on copy control recorded on the disk DK are obtained as a result of a series of processes wherein the information on copy control is superposed on an original digital video signal as digital-watermark information and the digital video signal including the information on copy control are subsequently compressed in accordance with the MPEG system and then encrypted in accordance with the CSS system.

[0151]

The readout unit 311 employed in the disk reproducing apparatus 31 reads out the information on the media type T_j and the digital video signal V_i from the

disk DK mounted on the disk reproducing apparatus 31. The information on the media type Tj and the digital video signal Vi are then supplied to the data processing unit 32 through the transmission line 33.

[0152]

In addition, the information on the media type Tj read out by the readout unit 311 is supplied to the media-type encrypting unit 312 also employed in the disk reproducing apparatus 31. Also this second embodiment, the information on the media type Tj is encrypted in accordance with the CSS system, being converted into encrypted information on the media type STj. Then, the encrypted information on the media type STj is also supplied to the data processing unit 32 through the transmission line 33.

[0153]

In the data processing unit 32, the encrypted information on the media type STj and the digital video signal Vi are supplied to the decryption unit 322 whereas the information on the media type Tj is supplied to the media-type decoding unit 321 as is the case with the information-signal reproducing system implemented by the first embodiment described earlier.

[0154]

The decryption unit 322 decrypts the encrypted digital video signal V_i and the encrypted information on the media type ST_j to produce a decrypted digital video signal V_m and decrypted information on the media type M_t . The digital video signal V_m is supplied to the MPEG decoding unit 323 and the information on the media type M_t is supplied to the media-type decoding unit 321.

[0155]

The MPEG decoding unit 323 decompresses the digital video signal V_m which has been compressed in accordance with the MPEG system to restore the original digital video signal V . The restored original digital video signal V is supplied to the digital-watermark-information detecting unit 324.

[0156]

Much like the digital-watermark-information detecting unit 124 employed in the first embodiment described above, the digital-watermark-information detecting unit 324 detects the type of the information on copy control superposed as digital-watermark information on the digital video signal received from the MPEG decoding unit 323. To put in detail, the digital-watermark-information detecting unit 324 determines whether the information on copy control is the copy-free

control information allowing copy operations to be carried out freely, the one-copy control information allowing the first-generation copy to be produced, the no-more-copy control information allowing no further generation copies or the never-copy control information absolutely prohibiting copy operations.

[0157]

In the mean time, the media-type decoding unit 321 decodes the information on the media type Tj received from the disk reproducing apparatus 31 and the decrypted information on the media type Mt received from the decryption unit 322 to detect information indicating whether the disk DK mounted on the disk reproducing apparatus 31 is a ROM or RAM disk, supplying the detected information on the disk type to the control-signal generating unit 325.

[0158]

At that time, if the information on the media type Tj is different from the decrypted information on the media type Mt or one of them is missing, the information on the media type is determined to have been altered. In this case, a request to inhibit a reproduction operation is output by the media-type decoding unit 321 to the control-signal generating unit 325.

[0159]

Receiving the request to inhibit a reproduction operation from the media-type decoding unit 321, the control-signal generating unit 325 generates a control signal to stop the operation to read out the digital video signal from the disk DK in the disk reproducing apparatus 31, supplying the control signal to the control-signal encrypting unit 326.

[0160]

If information on the media type is received from the media-type decoding unit 321 instead of the request to inhibit a reproduction operation, on the other hand, the control-signal generating unit 325 makes a determination as to whether or not the digital video signal recorded on the disk DK has been obtained as a result of an illegal copy operation. The determination is based on the information on the media type received from the media-type detecting unit 321 and the information on copy control detected by the digital-watermark-information detecting unit 324. If the digital video signal recorded on the disk DK is determined to have been obtained as a result of an illegal copy operation, a control signal to halt an operation to read out the digital video signal from the disk DK in the disk

reproducing unit 31 is generated and outputted to the control-signal encrypting unit 326.

[0161]

To be more specific, if the information on the media type received by the control-signal generating unit 325 from the media-type decoding unit 321 indicates that the disk DK is a ROM disk and the information on copy control is the no-more-copy control information, or the information on the media type received from the media-type decoding unit 321 indicates that the disk DK is a RAM disk and the information on copy control is the never-copy or one-copy control information, a control signal to halt the operation to read out the digital video signal from the disk DK is generated and supplied to the control-signal encrypting unit 326.

[0162]

If the information on the media type indicates that the disk DK is a ROM disk and the information on copy control is the never-copy or one-copy control information, or the information on the media type indicates that the disk DK is a RAM disk and the information on copy control is the no-more-copy control information, a control signal to continue the operation to read out the digital video signal from the disk DK is generated and supplied to the

control-signal encrypting unit 326.

[0163]

The control-signal encrypting unit 326 encrypts the control signal received from the control-signal generating unit 325 in accordance with the CSS system and transmits the encrypted control signal to the control-signal decrypting unit 313 employed in the disk reproducing apparatus 31.

[0164]

The control-signal decrypting unit 313 employed in the disk reproducing apparatus 31 decrypts the encrypted control signal by using the same algorithm as an algorithm for the encryption carried out by the control-signal encrypting unit 326 employed in the data processing unit 32 or a correct encryption key to produce a decrypted control signal which is then supplied to the readout control unit 314. If the control-signal decrypting unit 313 is not capable of normally decrypting the encrypted control signal, the control signal is determined to be abnormal. In this case, a control signal to halt the operation to read out the digital video signal from the disk DK is generated and supplied to the readout control unit 314.

[0165]

The readout control unit 314 controls the operation to read out the digital video signal from the disk DK in accordance with the control signal received from the control-signal decrypting unit 313. If the encrypted control signal received from the data processing unit is a control signal to halt the operation to read out the digital video signal from the disk DK, the readout control unit 314 controls the readout unit 311 or a disk driving unit not shown in the figure to halt the operation to read out the digital video signal from the disk DK.

[0166]

As described above, if the control-signal decrypting unit 313 is not capable of normally decrypting the encrypted control signal transmitted from the data processing unit 32 because for example the control signal has been altered during the transmission, a control signal to halt the operation to read out the digital video signal from the disk DK is generated and supplied to the readout control unit 314. Also in this case, the readout control unit 314 controls the readout unit 311 to halt the operation to read out the digital video signal from the disk DK.

[0167]

As described above, the data processing unit 32 is capable of correctly and reliably making a determination as to whether or not a digital video signal recorded on the disk DK has been obtained as a result of an illegal copy operation by considering unencrypted information on the media type Tj, encrypted information on the media type STj and information on copy control superposed on the digital video signal as digital-watermark information which are received from the disk reproducing information 31.

[0168]

On the basis of the outcome of the determination, the disk reproducing apparatus 31 can be controlled to disable the operation itself to read out the digital video signal from the disk DK. Thus, it is possible to reliably prevent the use of a digital video signal which has been obtained as a result of an illegal copy operation.

[0169]

In addition, in the case of the information-signal reproducing system 30 implemented by the second embodiment, digital video signal Vi read out from the disk DK, information on the media type Tj and encrypted information on the media type STj are transmitted from

the disk reproducing information 31 to the data processing unit 32 while an encrypted control signal is transmitted from the data processing unit 32 to the disk reproducing apparatus 31.

[0170]

Accordingly, in the information-signal reproducing system implemented by the second embodiment, both the encrypted information on the media type and the encrypted control signal must be decrypted. Thus, an attempt to reproduce a digital video signal obtained as a result of an illegal copy operation such as alteration of the encrypted information on the media type or the encrypted control signal will cause the operation of reading out the digital video signal from the disk to be disabled. It is therefore possible to reliably prevent the use of the digital video signal obtained as a result of an illegal copy operation. That is to say, the information-signal reproducing system is capable of improving the reliability of the reproduction control to prevent the use of the digital video signal obtained as a result of an illegal copy operation.

[0171]

In addition, in the information-signal reproducing system implemented by the second embodiment, the

operation to reproduce a digital video signal from the disk DK is halted by the disk reproducing apparatus 31 which supplies the digital video signal to the data processing unit 32. Thus, it is possible to impose reproduction restrictions for protection of a copyright with a higher degree of security.

[0172]

(Modification of the Second Embodiment)

As described above, information on copy control may be superposed in digital-watermark processing on an elementary stream obtained as a result of an MPEG encoding process of the digital video signal. In this case, by designing an information-signal reproducing system like one shown in FIG. 5 wherein the information on copy control superposed on the digital video signal as digital-watermark information can be detected from the digital video signal completing the MPEG encoding process, it is possible to impose restrictions on the operation to reproduce the digital video signal in the disk reproducing unit 31.

[0173]

In this case, a watermark-information detecting unit 411 employed in a data processing unit 41 of the information-signal reproducing system shown in FIG. 5 is

different from the watermark-information detecting unit 324 shown in FIG. 4. However, the other components are identical with their respective counterparts shown in FIG. 4. Components in FIG. 5 identical with their counterparts shown in FIG. 4 are denoted by the same reference numerals as the latter and their explanation is omitted.

[0174]

The watermark-information detecting unit 411 employed in a data processing unit 41 detects information on copy control superposed on the encoded digital video signal prior to the MPEG decoding process and supplies the detected type of the information on copy control to the output control-signal generating unit 325.

[0175]

As described above, even in the case of information on copy control superposed in digital-watermark processing on an elementary stream obtained as a result of an MPEG encoding process of the digital video signal, it is possible to reliably execute control of an operation to reproduce the digital video signal based on the information on the media type T_j and the encrypted information on the media type ST_j in the disk reproducing apparatus 31.

[0176]

In the second embodiment, the operation to read out an information signal in the disk reproducing apparatus is controlled so that, when the operation to read out an information signal in the disk reproducing apparatus is halted, the operation to output the video signal from the MPEG decoding unit can also be halted as well.

[0177]

In this case, the MPEG decoding unit can also be controlled directly. As an alternative, a switch circuit like the one employed in the first embodiment is provided for blocking or passing on the video signal output by the MPEG decoding unit to external equipment.

[0178]

In addition, a control signal for controlling the operation to read out the video signal in the disk reproducing apparatus is generated and encrypted in the data processing unit before being supplied to the disk reproducing apparatus as described above. It should be noted that the control signal can be supplied to the disk reproducing apparatus without being encrypted.

[0179]

In the descriptions of the first and second embodiments, information on copyright protection is exemplified by information on the media type. It should

be noted, however, that the information on copyright protection is not limited to the information on the media type. For example, as information on copyright protection, information on a term of validity to use a main information signal can be added to a recording medium in which the main information signal is recorded. The information on a term of validity is supplied by the disk reproducing apparatus to the data processing unit which can be executed to prevent the main information signal from being output if the term of validity is found expired.

[0180]

In this case, both encrypted information on a term of validity and unencrypted information on a term of validity are supplied to the data processing unit as is the case with the above-mentioned embodiments. If the former does not match the latter, the term of validity to use the main information signal is determined to have been altered. In this case, the operation to output the main information signal is halted.

[0181]

As described above, by controlling the processing to output the main information signal on the basis of the encrypted information on a copyright protection and the

unencrypted information on a copyright protection without taking the information on copy control into consideration, it is possible to reliably prevent the main information signal from being used illegally.

[0182]

Thus, by designing an apparatus for controlling the processing of a main information signal based on encrypted information on copyright protection and unencrypted information on copyright protection, it is possible to reliably prevent the main information signal from being used illegally. Of course, by also taking information such as the information on copy control as is the case with the embodiments described above in consideration, it is possible to even more reliably prevent the main information signal from being used illegally.

[0183]

In addition to information on a media type and information on a term of validity described above, as information on copyright protection, it is possible to use various kinds of information that may probably be altered in order to illegally use a main information signal. That is to say, as information on copyright protection, CGMS information used as information on copy

control or sub-code information of the main information signal such as a digital video signal can also be encrypted by the disk reproducing apparatus and supplied to the data processing unit.

[0184]

In this case, by comparing unencrypted sub-code information or unencrypted CGMS information with the encrypted sub-code information or the encrypted CGMS information respectively, it is possible to make a determination as to whether or not the sub-code information or CGMS information has been altered typically in an attempt to illegally copy the main information signal and, hence, to control the operation to reproduce the main information signal.

[0185]

In addition, in the embodiments described above, information on copy control is subjected to a spectrum-spreading process in order to generate digital-watermark information. It should be noted that the technique to create digital-watermark information is not limited to the spectrum-spreading process. That is to say, digital-watermark information can be created from information on copy control and superposed on a main information signal by adopting another digital-watermark technique. The

digital-watermark information is detected by using a method depending on the digital-watermark technique.

[0186]

Information on copy control for controlling copy operations is not limited to digital-watermark information. Other information on copy control such as CGMS information can also be used as well.

[0187]

In addition, in the embodiments described above, information on the media type and a control signal supplied by the data processing unit to the disk reproducing apparatus and used for controlling a read operation in the disk reproducing apparatus are encrypted in accordance with the CSS system. It should be noted that the encryption technique is not limited to that of the CSS system. A variety of encryption techniques can be adopted.

[0188]

To be more specific, in the case of the second embodiment, in the media-type encrypting unit 312 employed in the disk reproducing apparatus 31 and the control-information encrypting unit 326 employed in the data processing unit 32 or 42, the encryption technique of the CSS system or an encryption technique using an

entirely different algorithm or a different encryption key can be adopted. If the encryption technique adopted in the media-type encrypting unit 312 is different from the encryption technique adopted in the control-information encrypting unit 326, the security offered by the information-signal reproducing system can be further enhanced.

[0189]

In addition, in the embodiments described above, the video signal output by the data processing units 12, 21, 31 and 41 is supplied to a monitor receiver or a recording apparatus for recording the information signal. When the video signal output by the data processing units 12, 21, 31 and 41 is supplied to a recording apparatus, for example, it is possible to prevent a main information signal obtained as a result of an illegal copy operation from being further copied illegally since the video signal output by the data processing units 12, 21, 31 and 41 is not a signal obtained as a result of an illegal copy operation. That is to say, the copy control can be executed correctly as well as reliably. Furthermore, also in the case of a data processing unit provided with a facility of a recording apparatus, the copy control can be executed correctly as well as reliably so that a main

signal obtained as a result of an illegal copy operation is not copied again.

[0190]

In addition, in the embodiments described above, a digital video signal recorded on a DVD is reproduced. It should be noted, however, that the processed signal does not have to be a video signal. For example, it is needless to say that the processed signal can also be an audio signal, a variety of programs or various kinds of data. If the main control signal is a game program, for example, in the first embodiment described above, it is possible to execute control in the data processing unit to prevent the game program from being executed in case the program has been obtained as a result of an illegal copy operation.

[0191]

The processing of the main information signal controlled in the data processing unit includes various kinds of processing such as recording and execution of the main information signal in addition to the processing to output the main information signal explained in the descriptions of the embodiments.

[0192]

Furthermore, in the embodiments described above,

the disk recording medium is a DVD. It is worth noting, however, the recording medium is not limited to a DVD. For example, the recording medium can be a variety of magnetic optical disks and optical disks such as a CD (compact disk) and an MD (mini disk). That is to say, the present invention can be applied to an apparatus for reading out an information signal from such a disk and processing the signal.

[0193]

In addition, the disk reproducing apparatus and the data processing unit described above may be accommodated in a single cabinet like a DVD reproducing apparatus or a DVD recording apparatus, or each built as a standalone box. To be more specific, the disk reproducing apparatus and the data processing unit are presented respectively as a disk driver and the main body of a personal computer as described above. Of course, it is possible to present a disk driver (an information-signal reading apparatus) provided with the functions of the disk reproducing apparatuses 11 and 31 described earlier with reference to FIGS. 1 to 5 as a standalone unit.

[0194]

By the same token, it is of course possible to present an information-signal processing apparatus

provided with the functions of the data processing unites 12, 21, 31 and 41 described earlier with reference to FIGS. 1 to 5 as a standalone unit. The functions to be provided to the information-signal processing apparatus can be presented as software written in a so-called PC card which is used by mounting the card onto typically a personal computer implementing the apparatus. As an alternative, the functions to be provided to the information-signal processing apparatus can also be presented as an add-on board including circuits for implementing the functions. Such a board is plugged onto the information-signal processing apparatus to add the functions thereto.

[0195]

In addition, in the embodiments described above, the information-signal reproducing system provided by the present invention includes a DVD disk drive and a personal computer. It should be noted, however, that the information-signal reproducing system is not limited to such a configuration. For example, the present invention can also be applied to a system used in conjunction with the Internet or digital satellite broadcasting which serves as transmission media.

[0196]

In such a system, the disk reproducing apparatus for presenting a main information signal, information on the media type and encrypted information on the media type is implemented by a server. On the other hand, the data processing unit for receiving and processing these pieces of information is implemented by a client apparatus. In the system built in accordance with the present invention by using the Internet or digital satellite broadcasting as transmission media, it is possible to improve security against an operation to copy an information signal illegally.

[0197]

As described above, according to the information-signal reproducing system according to claim 1, both the information on copyright protection read out from the recording medium and encrypted information on copyright protection are used. Since the encrypted information on copyright protection is difficult to alter, it will be possible to determine whether or not the information on copyright protection has been altered in an attempt to reproduce the main information signal obtained as a result of an illegal copy operation. When thus discriminated being different from each other, a main information signal obtained as a result of an illegal

copy operation can be prevented from being reproduced with a high degree of reliability.

[0198]

Also, according to the information-signal reproducing system according to claim 2, it is difficult to alter the encrypted medium-type identification information, even though the unencrypted one read out from the disk can be altered. As a result, if the unencrypted medium-type identification information is found different from the encrypted medium-type identification information, the unencrypted information is determined to have been altered in an attempt to reproduce a main information signal resulting from an illegal copy operation. Thus, a main information signal obtained as a result of an illegal copy operation can be prevented from being reproduced with a high degree of reliability.

[0199]

Also, according to the information-signal reproducing system according to claim 3, it is difficult to alter the encrypted information on copyright protection, thereby the information on copyright protection is securely supplied from the information-signal reading system to the information-signal

processing apparatus. Thus, a main information signal obtained as a result of an illegal copy operation can be prevented from being reproduced with a high degree of reliability, on the basis of the information on copyright protection and the encrypted information on copyright protection.

[0200]

Also, according to the information-signal reproducing system according to claim 4, whether or not the information signal recorded on the recording medium is illegal copied is reliably determined, with consideration given to the additional information for controlling the copy operation added to the main information signal. Thereby the reproduction control of the information signal recorded on the recording medium is executed appropriately and reliably.

[0201]

Also, according to the information-signal reproducing system according to claim 5, the additional information for controlling a copy operation added as digital-watermark information on the main information signal is detected. In consideration of the additional information, the reproduction control of the main information signal can be executed more appropriately and

reliably.

[0202]

Also, according to the information-signal reproducing system according to claim 6, reproduction of illegally copied information signal by altering information on copyright protection can be prevented reliably. In this case, an operation itself to read out the main information signal from the recording medium is controlled, so that the reproduction of the main information signal is controlled reliably.

[0203]

Also, according to the information-signal reproducing system according to claim 7, for example, in an attempt to reproduce the main information signal obtained as a result of an illegal copy operation, both the encrypted information on copyright protection read out from the information-signal reading apparatus and the encrypted readout-control-signal supplied from the information-signal processing apparatus must be altered. However, since both of them are encrypted, it is difficult to alter them. Thus, the reliability for the information-signal reproducing system is further enhanced.

[0204]

Also, according to the information-signal

reproducing system according to claim 8, if the unencrypted information on the media type is different from the encrypted information on the media type, media-type information is determined to have been altered for reproduction of illegal-copied information-signal, so that information-signal reproducing apparatus can operate controlling for reading out the information signal appropriately and reliably.

[0205]

Also, according to the information-signal reproducing system according to claim 9, since the information on copyright protection can not be altered easily, the encrypted information on copyright protection is surely supplied from the information-signal reading apparatus to the information-signal processing apparatus. Thereby, in accordance with the information on copyright protection and encrypted information on copyright protection, the information-signal reading apparatus can operates readout process of the main information signal, appropriately and reliably.

[0206]

Also, according to the information-signal reproducing system according to claim 10, if the illegal copied information-signal on a recording medium is to be

reproduced, both the encrypted information on copyright protection and the readout-control signal are needed to be decrypted. Thus, the reliability for the information-signal reproducing system is enhanced.

[0207]

Also, according to the information-signal reproducing system according to claim 11, in accordance with the information on copyright protection and the additional information for copy control added to the main information signal, the information-signal reading apparatus operates control for readout process of information signal, appropriately and reliably.

[0208]

Also, according to the information-signal reproducing system according to claim 12, in accordance with the information on copyright protection and the additional information provided as digital-watermark information added to the main information, the information-signal reading apparatus operates control for readout process of information signal, appropriately and reliably.

[Brief Description of the Drawings]

[FIG. 1]

FIG. 1 is a block diagram used for explaining an embodiment implementing an information-signal reproducing system provided by the present invention.

[FIG. 2]

FIG. 2 is a block diagram used for explaining a digital-watermark-information detecting unit employed in the information-signal reproducing system shown in FIG. 1.

[FIG. 3]

FIG. 3 is a block diagram used for explaining a modification of the information-signal reproducing system shown in FIG. 1.

[FIG. 4]

FIG. 4 is a block diagram used for explaining another implementation of the information-signal reproducing system shown in FIG. 1.

[FIG. 5]

FIG. 5 is a block diagram used for explaining a modification of the information-signal reproducing system shown in FIG. 1.

[FIG. 6]

FIG. 6 is a block diagram used for explaining an information-signal recording apparatus for producing a disk recording medium for regularly recording an information signal.

[FIG. 7]

FIGS. 7A to 7D are diagrams used for explaining a relation between an information signal and an SS-information on copy control (digital-watermark information) superposed on the information signal.

[FIG. 8]

FIG. 8 is a block diagram used for explaining an information-signal reproducing system in which an operation to reproduce a main information signal from a disk is controlled by taking information on an attribute of a recording medium into consideration.

[FIG. 9]

FIG. 9 is a block diagram used for explaining an information-signal reproducing system capable of altering information on an attribute of a recording medium.

[Description of Reference Numerals]

11, 31 ... disk reproducing apparatus; 12, 32 ... data processing unit; 13, 33 ... transmission line; 111 ... readout unit; 112 ... media-type encrypting unit; 121 ... media-type decoding unit; 122 ... decryption unit; 123 ... MPEG decoding unit; 124, 211 ... digital-watermark-information detecting unit; 125 ... output control unit; 126 ... switch circuit; 311 ... readout unit; 312 ... media-type encrypting unit; 313 ... control-signal decrypting

unit; 314 ... readout control unit; 321 ... media-type
decoding unit; 322 ... decryption unit; 323 ... MPEG
decoding unit; 324, 411 ... digital-watermark-information
detecting unit; 325 ... control-signal generating unit; 326
... control-signal encrypting unit.

[Name of Document] Abstract of the Disclosure

[Abstract]

[Object] The present invention provides an apparatus and a method for protecting a copyright of a information signal with a high degree of reliability and for preventing a information signal from being copied illegally by substantially disabling an operation to reproduce a information signal obtained as a result of an illegal copy operation.

[Solving Means] A disk reproducing apparatus 11 reads out the digital video signal Vi as a main information signal from a disk DK and a media type Tj recorded on a TOC of the disk DK, then obtains a encrypted information on a media type STj generated by encrypting the media type Tj, and supplies Vi, Tj, and STj to a data processing unit 12. The data processing unit 12 determines whether or not the information signal is illegally copied, on the basis of the media type Tj and the encrypted information on the media type STj, thus controls reproduction of the digital video signal Vi recorded on the disk DK.

[Selected Drawing] FIG. 1

In the Drawings:

[FIG. 1]

10: Information-signal reproducing system (Information-signal reproducing apparatus)

112: Media-type encrypting unit

111: Readout unit

11: Disc reproducing apparatus

121: Media-type decoding unit

122: Decrypting unit

123: MPEG decoding unit

124: Digital-watermark-information detecting unit

125: Output control unit

12: Data processing unit

[FIG. 2]

244: Code identifier

242: Synchronization detecting unit

243: PN-code generating unit

[FIG. 3]

20: Information-signal reproducing system (Information-signal reproducing apparatus)

112: Media-type encrypting unit

111: Readout unit

11: Disc reproducing apparatus
121: Media-type decoding unit
122: Decrypting unit
123: MPEG decoding unit
211: Digital-watermark-information detecting unit
125: Output control unit
21: Data processing unit

[FIG. 4]

30: Information-signal reproducing system (Information-signal reproducing apparatus)
312: Media-type encrypting unit
311: Readout unit
31: Disc reproducing apparatus
314: Readout control unit
313: Control-signal decrypting unit
321: Media-type decoding unit
322: Decrypting unit
323: MPEG decoding unit
324: Digital-watermark-information detecting unit
325: Control-signal generating unit
326: Control-signal encrypting unit
32: Data processing unit

[FIG. 5]

40: Information-signal reproducing system (Information-signal reproducing apparatus)
312: Media-type encrypting unit
311: Readout unit
31: Disc reproducing apparatus
314: Readout control unit
313: Control-signal decrypting unit
321: Media-type decoding unit
322: Decrypting unit
323: MPEG decoding unit
411: Digital-watermark-information detecting unit
325: Control-signal generating unit
326: Control-signal encrypting unit
41: Data processing unit

[FIG. 6]

50: Recording apparatus
55: Data compressing unit
56: Encryption unit
58: Write unit
57: Media-type generating unit
541: PN-code generating unit
542: Information on copy control generating unit

544: Level control unit

[FIG. 7]

(a): Information on copy control spectrum before a spectrum-spreading process

(b): Information on copy control spectrum after a spectrum-spreading process

(c): Spectrum of an information signal with SS-information on copy control superposed thereon

A: Information signal

B: Dynamic range of the information signal

C: SS-information on copy control

D: Information on copy control

E: Information signal

(d): Signal spectrum after a spectrum-inverse-spreading process

[FIG. 8]

100: Information-signal reproducing system (Information-signal reproducing apparatus)

104: Readout unit

101: Disc reproducing apparatus

105: Media-type decoding unit

106: Digital-watermark-information detecting unit

107: Output control unit

102: Data processing unit

[FIG. 9]

200: Illegal reproducing system

104: Readout unit

101: Disc reproducing apparatus

105: Media-type decoding unit

106: Digital-watermark-information detecting unit

107: Output control unit

102: Data processing unit

201: Media-type altering apparatus

る。また、この情報処理装置が備えるべき機能は、例えば、パーソナルコンピュータ本体などに接続して使用されるいわゆるPCカードなどにより、ソフトウェアとして提供するようにすることもできる。前述の情報処理装置が備えるべき機能を実現する回路を搭載した増設ボードなどにより、情報信号処理装置に追加するようにすることもできる。

[0195]
また、前述の実施の形態においては、この発明による情報信号再生システムをDVDのデジタルメディアと、パーソナルコンピュータとにより構成されるものとして説明したが、これに限るものではない。例えば、インターネットやデジタル衛星放送を伝送媒体としたシステムに適用してもよい。

[0196]
この場合には、主情報信号、メタデータ情報、暗号化メタデータ情報を再生するデコーダ再生部が、サブ装置となり、これらの情報提供を受けて出力するようにするデータ処理部がクライアント装置となるシステムが構成される。このようにすることによって、インターネットやデジタル放送を伝送媒体とするシステムでは、情報信号の違法な複製に對してセキュリティを高くすることができ。

[0197]
[発明の効果]

以上説明したように、請求項1に記載の発明の情報信号再生システムによれば、記録媒体から読み出された著作権保護に関する情報と、改ざんすることが難しい暗号化された著作権保護に関する情報とを用いることによって、両者が同じでないときには、違法に複製された情報信号を再生するために、著作権保護に關する情報が改ざんされたと判断し、違法に複製された情報信号の再生を確実に防止することができる。

[0198]
また、請求項2に記載の発明の情報信号再生システムによれば、暗号化されずに提供された媒体識別情報を改ざんすることができても、暗号化されて提供された媒体識別情報は改ざんすることが難しいので、両媒体識別情報が同じでないときには、違法に複製された情報信号を再生するために、媒体識別情報が改ざんされたと判断し、違法に複製された情報信号の再生を確実に防止することができる。

[0199]
また、請求項3に記載の発明の情報信号再生システムによれば、暗号化された著作権保護に関する情報は簡単に改ざんすることができないようにされるので、著作権保護に関する情報を複製し、複製された情報信号が暗号化されている状態に提供されることができ、これにより、著作権保護に關する情報が改ざんされた著作権複製に関する情報とに基づいて、違法に複製された情報信号の再生を確実に防止することができる。

[0200]
また、請求項4に記載の発明の情報信号再生システムによれば、主情報信号に付加されている複製制御用の付加情報をも考慮して、記録媒体に記録されている情報信号は、違法に複製されたものか否かを複製に判別し、記録媒体に記録されている情報信号の再生制御を適正かつ複製に行うことができる。

[0201]
また、請求項5に記載の発明の情報信号再生システムによれば、主情報信号に電子透かし情報として付加されている複製制御用の付加情報を検出し、この付加情報をも考慮することによって、主情報信号の再生制御をより適正かつ複製に行うことができる。

[0202]
また、請求項6に記載の発明の情報信号再生システムによれば、著作権保護に関する情報を改ざんすることにより行なわれる違法に複製された情報信号の再生を確実に防止することができる。この場合、記録媒体からの主情報信号の読み出し自体が制御されるので、複製に主情報信号の再生を制御することができる。

[0203]
また、請求項7に記載の発明の情報信号再生システムによれば、違法に複製した情報信号を再生しようとする場合には、情報信号読み出し装置からの暗号化された著作権保護に関する情報と、情報信号処理装置からの暗号化された読み出し制御情報との両方を改ざんしなければならないが、両方とも暗号化されているので改ざんは難しく、情報信号再生システムに対する信頼性をさらに高めることができる。

[0204]
また、請求項8に記載の発明の情報信号再生システムによれば、暗号化されずに提供された媒体識別情報と、暗号化されて提供された媒体識別情報とが同じでないときには、違法に複製された情報信号を再生するために、媒体識別情報が

改ざんされたと判断し、情報信号再生装置においての情報信号の読み出し動作を適正かつ複製に行うことができる。

[0205]
また、請求項9に記載の発明の情報信号再生システムによれば、著作権保護に関する情報は簡単に改ざんすることができないようにされるので、暗号化された著作権保護に関する情報を複製し、複製された情報信号が暗号化されている状態に提供されることができ、これにより、著作権保護に關する情報が改ざんされた著作権複製に関する情報とに基づいて、違法に複製された情報信号の再生を確実に防止することができる。

[0206]
また、請求項10に記載の発明の情報信号再生システムによれば、違法に記録媒体に記録した情報信号を再生して利用使用とする場合には、暗号化された著作権保護に関する情報と、暗号化された読み出し制御情報との両方を暗号解除する必要があるため、情報信号再生システムの信頼性を向上させることができる。

[0207]
また、請求項11に記載の発明の情報信号再生システムによれば、著作権保護に關する情報と、主情報信号に付加されている複製制御用の付加情報とに基づいて、情報信号読み出し装置においての情報信号の読み出し動作の制御を適正かつ複製に行うことができる。

[0208]
また、請求項12に記載の発明の情報信号再生システムによれば、著作権保護に關する情報と、主情報信号に付加されている電子透かし情報として提供される付加情報とに基づいて、情報信号読み出し装置においての情報信号の読み出し動作を適正かつ複製に制御することができる。

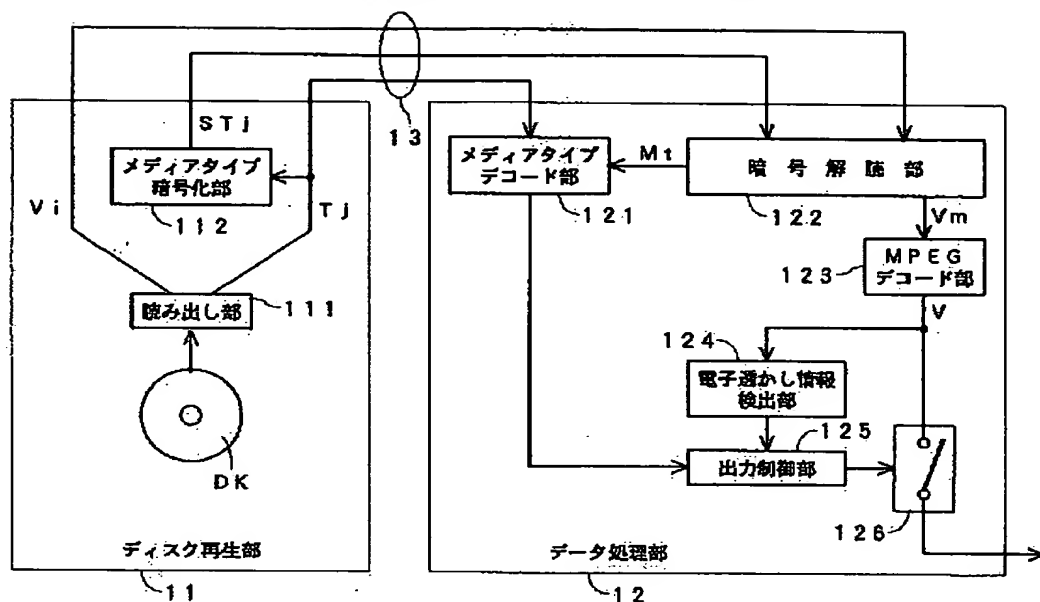
[図面の簡単な説明]
[図1]
この発明による情報信号再生システムの一実施の形態を説明するためのブロック図である。
[図2]
図1に示した情報信号再生システムの電子透かし情報検出装置を説明するためのブロック図である。
[図3]
図1に示した情報信号再生システムの変形例を説明するためのブロック図である。

[図4]
この発明による情報信号再生システムの他の例を説明するためのブロック図である。
[図5]
図1に示した情報信号再生システムの変形例を説明するためのブロック図である。

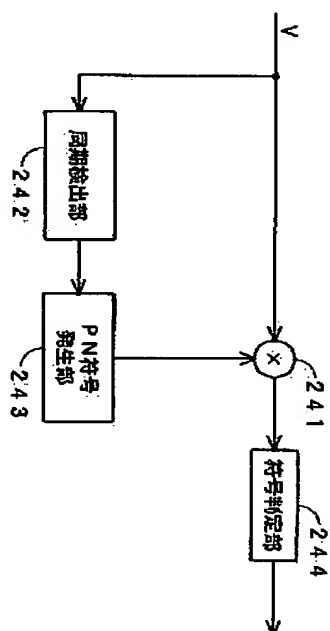
[図6]
正規に情報信号を記録したデジタル記録媒体を作成する情報信号記録装置を説明するためのブロック図である。
[図7]
情報信号とこれに重畳されるSS複製制御情報（電子透かし情報）の関係を説明するための図である。
[図8]
媒体属性情報をも考慮してデジタルに記録されている主情報信号の再生を制御するようにする情報信号再生システムを説明するためのブロック図である。

[図9]
媒体属性情報の改ざんが可能なされた情報信号再生システムを説明するためのブロック図である。
[符号の説明]
1、31…デジタル再生部、12、32…データ処理部、13、33…放送機（BS）、111…読み出し部、112…メタデータ暗号化部、121…メタデータデコード部、122…暗号解読部、123…MP E Gデコード部、124、211…電子透かし情報検出部、125…出力制御部、126…スライツチ回路、311…読み出し部、312…メタデータ暗号化部、313…制御情報暗号解読部、314…読み出し制御部、321…メタデータデコード部、322…暗号解読部、323…MP E Gデコード部、324、411…電子透かし情報検出部、325…制御情報生成部、326…制御情報暗号化部
[発明名] 図面
[図1]

10 情報信号再生システム (情報信号再生装置)

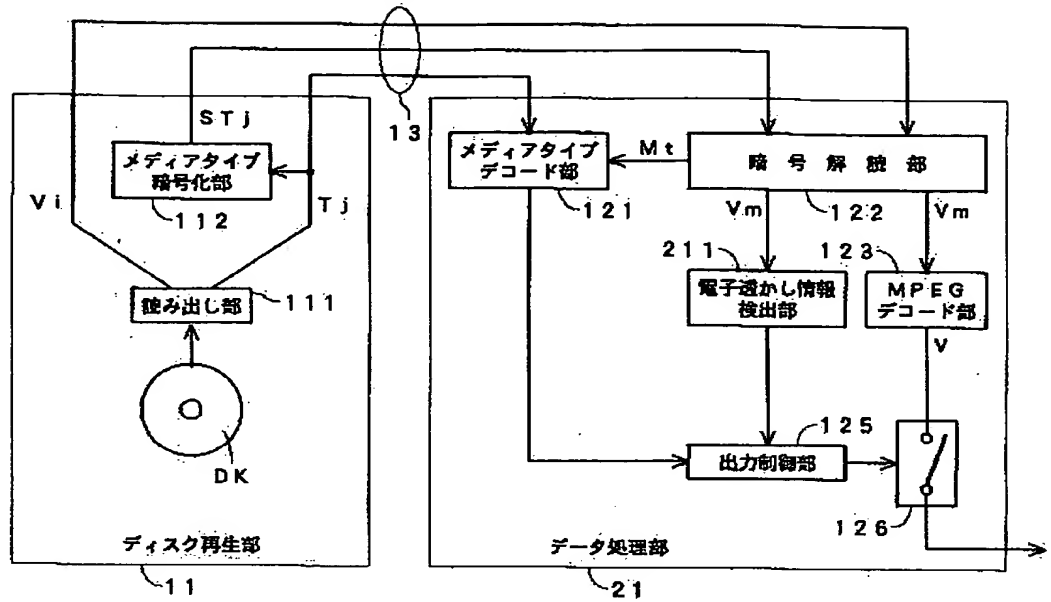


【例 3】



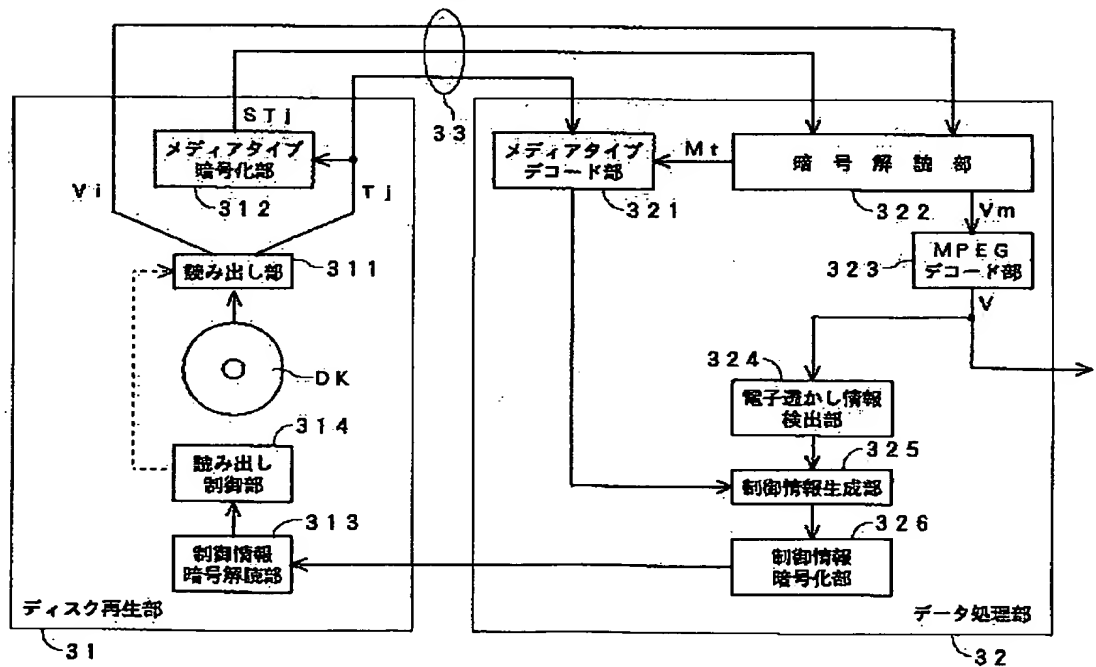
【図4】

2.0 情報信号再生システム (情報信号再生装置)



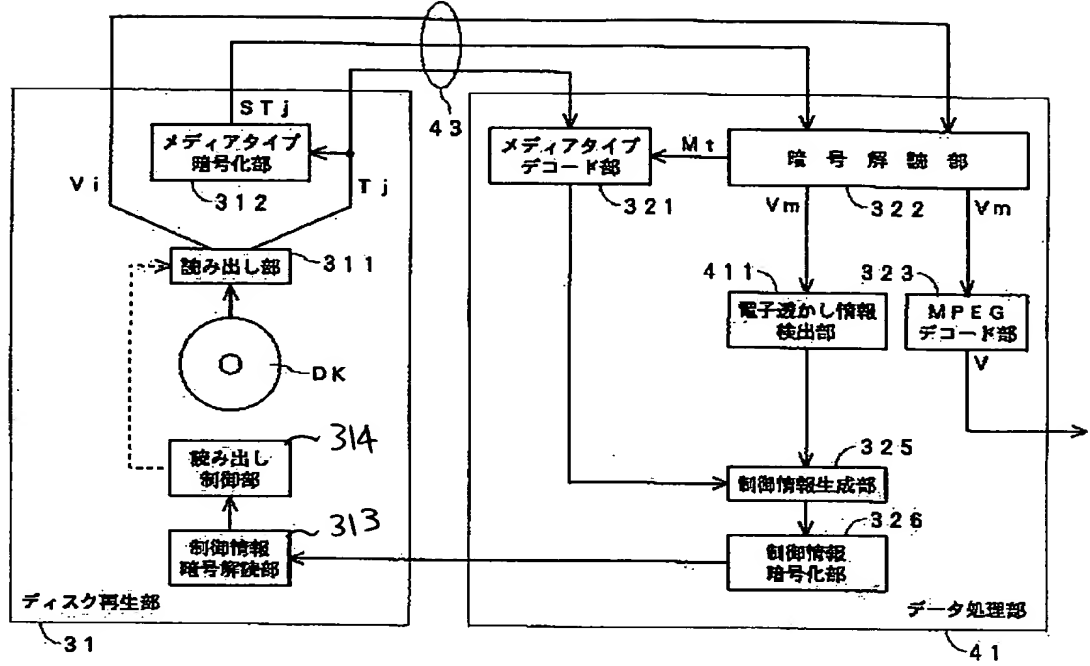
【図5】

3.0 情報信号再生システム (情報信号再生装置)



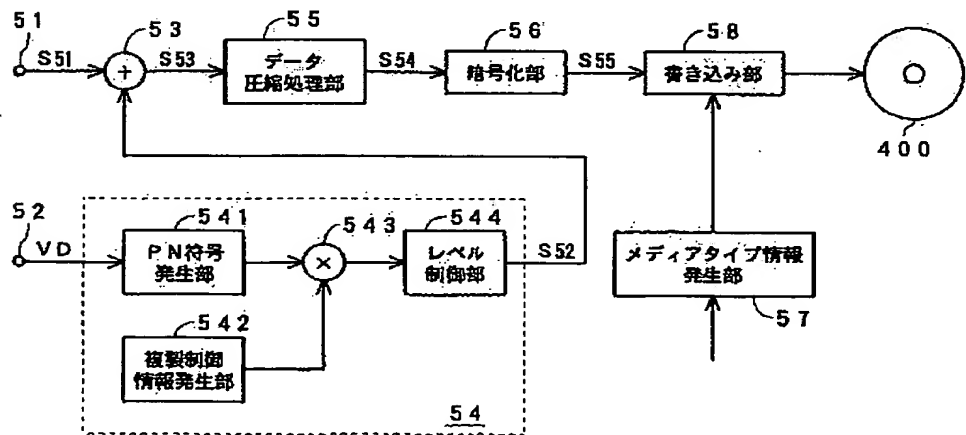
【図6】

40 情報信号再生システム（情報信号再生装置）

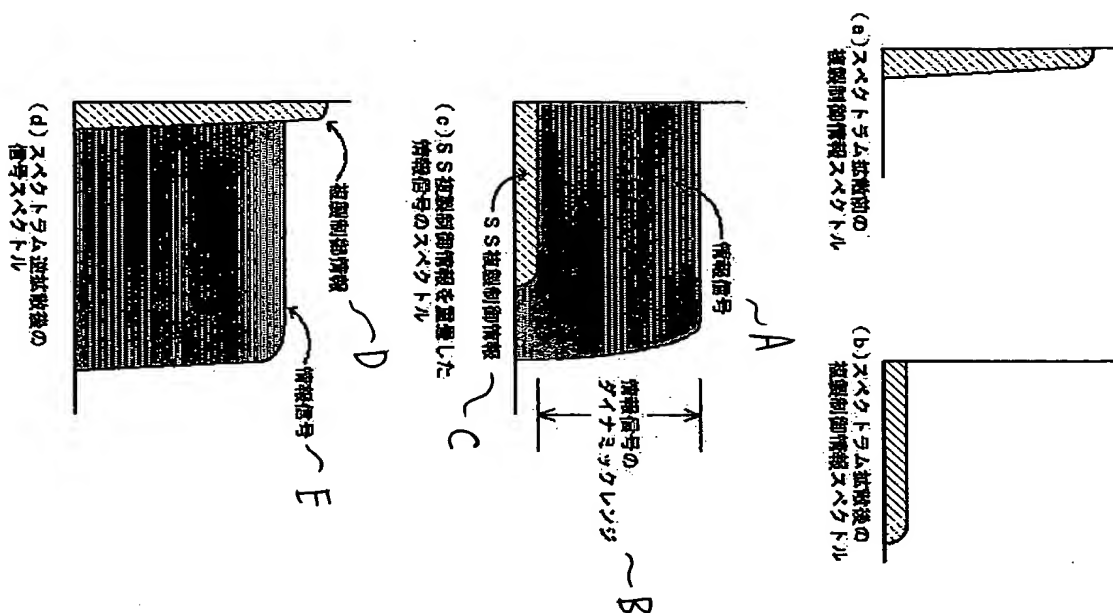


【図7】

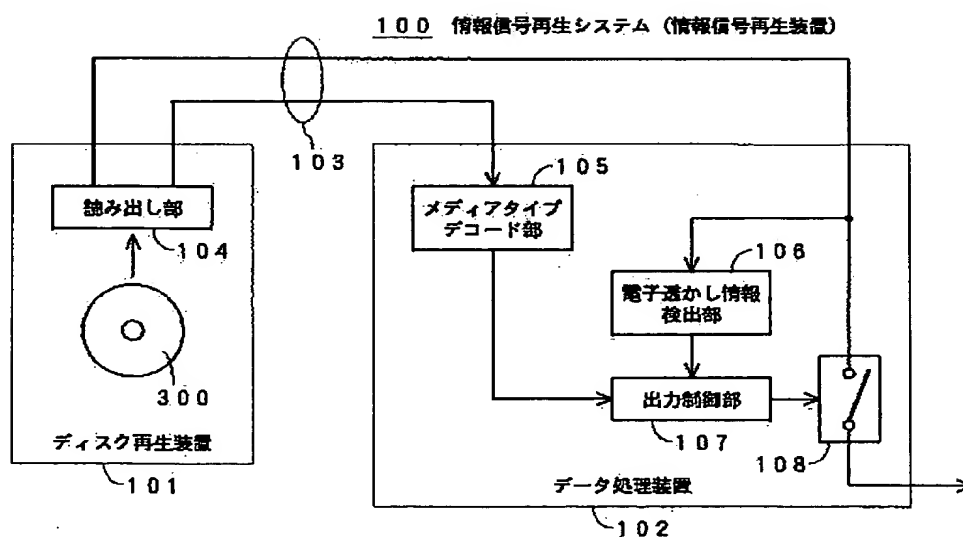
50 記録装置



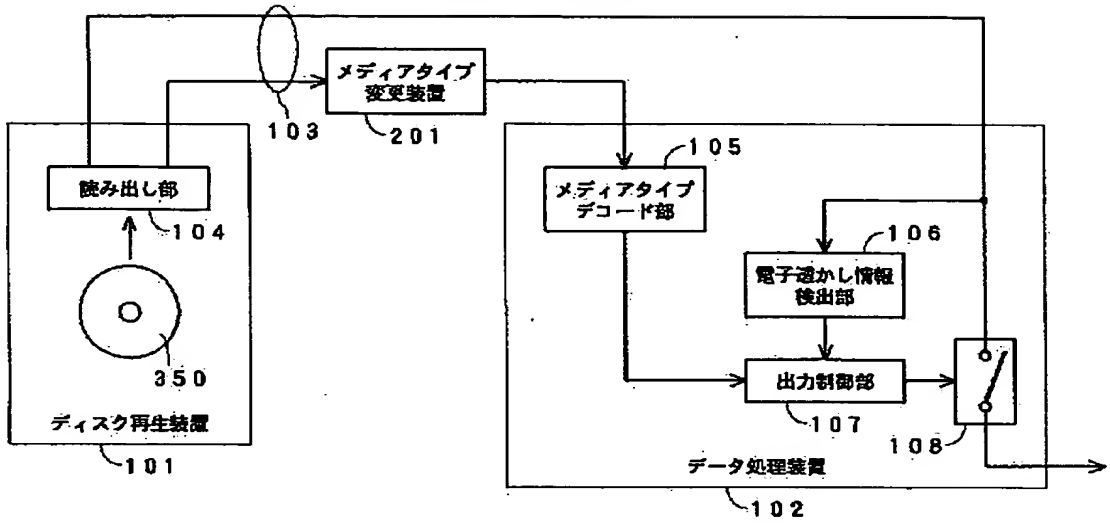
【図8】



【図9】



200 不正再生装置



要約書

【発明】 違法に記録媒体に記録された情報番号の再生を実質的に不能にすることにより、情報番号に係る著作権の適度な保護、情報番号の違法な複製を防止することのできる装置および方法を提供する。
 【解決手段】 ディスク再生部11は、ディスクから読み出した主情報番号

としてのデジタル映像番号V1と、ディスクのTOCに記録されている媒体属性情報（メディアタイプ情報）T1とを加えて、メディアタイプ情報を暗号化することにより形成した暗号化メディアタイプ情報ST1をデータ処理部12に供給する。データ処理部12においては、メディアタイプ情報T1と暗号化メディアタイプ情報ST1とに基づいて、違法に複製された情報番号を再生しようとしているか否かを判別し、ディスクに記録されているデジタル映像番号V1の再生制御を行う。
 図1

【選択図】